目　录

第一篇　代数结构

第二篇　组合数学

(7) $A^A = \{f \mid f: A \to A\}$，则函数的合成运算是 A^A 上的二元运算.

可以把二元运算的概念推广到 n 元运算.

定义 1.2　设 A 为集合，n 为正整数，$A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{个}}$表示 A 的 n 阶笛卡儿积. 函数 $f: A^n \to A$ 称为 A 上的一个 **n 元代数运算**，简称为 **n 元运算**. 若 f 是 A 上的运算，也可以称 A 在运算 f 下是**封闭的**.

【例 1.2】

(1) 求一个数的相反数是整数集 Z，有理数集 Q，实数集 R 上的一元运算.

(2) 求一个 n 阶($n \geqslant 2$) 实矩阵的转置矩阵是 $M_n(R)$ 上的一元运算，而求逆阵不是 $M_n(R)$ 上的一元运算.

(3) 如果令 B 为全集，则集合的绝对补运算 $\sim$ 是 $P(B)$ 上的一元运算.

(4) 令 $R(B)$ 为集合 B 上的所有二元关系的集合，则关系的逆运算是 $R(B)$ 上的一元运算.

(5) 设 A 为集合，S 是所有从 A 到 A 的双射函数构成的集合，则求反函数的运算是 S 上的一元运算.

(6) R 为实数集，令 $f: R^n \to R$，$\forall \langle x_1, x_2, \cdots, x_n \rangle \in R^n$ 有 $f(\langle x_1, x_2, \cdots, x_n \rangle) = x_3$，则 f 是 R 上的 n 元运算. 它就是求一个 n 维向量的第三个分量的运算.

为了书写的方便，可以用**算符**来表示 n 元运算. 常用的算符有$\circ$，$*$，$\cdot$，$\square$，$\triangle$，$\cdots$. 如果用算符$\circ$表示例 1.2(6) 中的 n 元运算，则有

$$\circ(x_1, x_2, \cdots, x_n) = x_3.$$

当$\circ$表示二元运算时，常将算符$\circ$放在两个运算数之间，把$\circ(x_1, x_2)$ 记为 $x_1 \circ x_2$. 而对于一元运算$\triangle$，通常将后面运算数 x 的括号省略，简记为 $\triangle x$.

当 A 为有穷集时，A 上的一元和二元运算可以用**运算表**来给出．设 $A=\{a_1,a_2,\cdots,a_n\}$，$\circ$ 和 $\vartriangle$ 分别为 A 上的二元和一元运算，它们的运算表给在表 1.1.

表 1.1

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1\circ a_1$	$a_1\circ a_2$	$\cdots$	$a_1\circ a_n$
a_2	$a_2\circ a_1$	$a_2\circ a_2$	$\cdots$	$a_2\circ a_n$
$\vdots$				
a_n	$a_n\circ a_1$	$a_n\circ a_2$	$\cdots$	$a_n\circ a_n$

$\vartriangle$	$\vartriangle a_i$
a_1	$\vartriangle a_1$
a_2	$\vartriangle a_2$
$\vdots$	$\vdots$
a_n	$\vartriangle a_n$

【例 1.3】 设 $B=\{1,2\}$，$P(B)$ 上的二元运算 $\oplus$ 和一元运算 $\sim$ 的运算表如表 1.2 所示。

表 1.2

$\oplus$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\varnothing$

$\sim$	
$\varnothing$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\varnothing$

下面讨论二元运算的性质.

定义 1.3 设 A 为集合，$\circ$ 为 A 上的二元运算.

(1) 若 $\forall x,y\in A$ 有 $x\circ y=y\circ x$，则称 $\circ$ 运算在 A 上是**可交换的**，也称 $\circ$ 运算在 A 上满足**交换律**.

(2) 若 $\forall x,y,z\in A$ 有 $(x\circ y)\circ z=x\circ(y\circ z)$，则称 $\circ$ 运算在 A 上是**可结合的**，也称 $\circ$ 运算在 A 上满足**结合律**.

(3) 若 $\forall x\in A$ 有 $x\circ x=x$，则称 $\circ$ 运算在 A 上是**幂等的**，也称 $\circ$ 运算在 A 上满足**幂等律**.

【例 1.4】

(1) 实数集 R 上的加法和乘法是可交换的、可结合的，而减法不满足交换律和结合律.

(2) $M_n(R)(n \geqslant 2)$ 上的矩阵加法是可交换的、可结合的，而矩阵乘法是可结合的，但不是可交换的.

(3) $P(B)$ 上的并、交，对称差运算是可交换的、可结合的.

(4) A^A 上的函数合成运算是可结合的，但一般不是可交换的.

以上所有的运算中只有集合的并和交运算满足幂等律，其它的运算一般说来都不是幂等的.

某些二元运算$\circ$尽管不满足幂等律，但存在着某些元素 x 满足 $x \circ x = x$，称这样的 x 是关于$\circ$运算的**幂等元**. 例如实数集中，0 是加法的幂等元，0 和 1 是乘法的幂等元. 不难看出，如果集合中的所有元素都是关于$\circ$运算的幂等元，则$\circ$运算满足幂等律.

定义 1.4 设$\circ$为 A 上的二元运算，如果对于 A 中任取的 n 个元素 $a_1, a_2, \cdots, a_n, n \geqslant 3$，在 $a_1 \circ a_2 \circ \cdots \circ a_n$ 中任意加括号所得的运算结果都相等，则称$\circ$运算在 A 上是**广义可结合的**，或称$\circ$运算在 A 上适合**广义结合律**.

对于适合广义结合律的二元运算$\circ$，通常用 $a_1 \circ a_2 \circ \cdots \circ a_n$ 来表示 $a_1, a_2, \cdots, a_n$ 的运算结果.

定理 1.1 设$\circ$为 A 上的二元运算，若$\circ$运算适合结合律，则$\circ$运算适合广义结合律.

证 任取 A 中 n 个元素 $a_1, a_2, \cdots, a_n$，令

$$b = ((\cdots(((a_1 \circ a_2) \circ a_3) \circ a_4) \circ \cdots) \circ a_{n-1}) \circ a_n.$$

我们只须证明在 $a_1 \circ a_2 \circ \cdots \circ a_{n-1} \circ a_n$ 中任意加括号所得的运算结果都等于 b. 施归纳于 n.

$n = 3$，由结合律有 $(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3)$.

假设小于 n 时结论为真，对于 $a_1 \circ a_2 \circ \cdots \circ a_{n-1} \circ a_n$ 任意加括号后所得的运算结果是 c，且最后一次运算是在 α 和 β 两部分之间进行的. 根据归纳假设有 $\beta = (\cdots) \circ a_n$，代入 c 得

$$c = \alpha \circ ((\cdots) \circ a_n).$$

由结合律　$c = (\alpha \circ (\cdots)) \circ a_n$. 再使用归纳假设得

$$a\circ(\cdots) = (\cdots((a_1\circ a_2)\circ a_3)\circ\cdots)\circ a_{n-1}.$$

所以有

$$c = ((\cdots((a_1\circ a_2)\circ a_3)\circ\cdots)\circ a_{n-1})\circ a_n. \qquad \blacksquare$$

以上讨论的运算性质只涉及一个二元运算. 下面考虑与两个二元运算相关的性质，即分配律和吸收律.

定义 1.5 设$\circ$和 $*$ 是集合 A 上的二元运算.

(1) 若$\forall x,y,z\in A$有$x\circ(y*z)=(x\circ y)*(x\circ z)$和$(y*z)\circ x=(y\circ x)*(z\circ x)$成立，则称$\circ$运算对 $*$ 运算是**可分配的**，或称$\circ$运算对 $*$ 运算满足**分配律**.

(2) 若$\circ$和 $*$ 满足交换律且$\forall x,y\in A$有$x\circ(x*y)=x$和$x*(x\circ y)=x$成立，则称$\circ$和 $*$ 运算是**可吸收的**，或称$\circ$和 $*$ 运算满足**吸收律**.

【例 1.5】

(1) 实数集 R 上的乘法对加法是可分配的，但加法对乘法不满足分配律.

(2) n 阶($n\geqslant 2$)实矩阵集合 $M_n(R)$ 上的矩阵乘法对矩阵加法是可分配的.

(3) 幂集 $P(B)$ 上的并和交是互相可分配的，并且满足吸收律.

除了算律以外，还有一些和二元运算有关的特异元素，如单位元、零元、逆元等.

定义 1.6 设$\circ$为集合 A 上的二元运算.

(1) 若存在$e_l\in A$(或$e_r\in A$)使得$\forall x\in A$都有$e_l\circ x=x$(或$x\circ e_r=x$)，则称e_l(或e_r)是 A 中关于$\circ$运算的**左(或右)单位元**. 若$e\in A$关于$\circ$运算既为左单位元又为右单位元，则称e为 A 中关于$\circ$运算的**单位元**①.

(2) 若存在$\theta_l\in A$(或$\theta_r\in A$)使得$\forall x\in A$都有$\theta_l\circ x=\theta_l$(或$x\circ\theta_r$

① 在有的书中称单位元为幺元.

$= \theta_r$)，则称 θ_l(或 θ_r) 是 A 中关于$\circ$运算的**左(或右)零元**. 若 $\theta \in A$ 关于$\circ$运算既为左零元又为右零元，则称 θ 为 A 中关于$\circ$运算的**零元**.

【例 1.6】

(1) 整数集 Z 中关于加法的单位元是 0，没有零元，关于乘法的单位元是 1，零元是 0.

(2) n 阶($n \geqslant 2$) 实矩阵集合 $M_n(R)$ 中关于矩阵加法的单位元是 n 阶全 0 矩阵，没有零元，而关于矩阵乘法的单位元是 n 阶单位矩阵，零元是 n 阶全 0 矩阵.

(3) 幂集 $P(B)$ 中关于并运算的单位元是$\varnothing$，零元是 B，而关于交运算的单位元是 B，零元是$\varnothing$.

(4) A^A 中关于函数合成运算的单位元是 A 上的恒等函数 I_A，$I_A: A \to A, I_A(x) = x, \forall x \in A$. 没有零元.

(5) $A = \{a_1, a_2, \cdots, a_n\}$，$n \geqslant 2$. 定义 A 上的二元运算$\circ$，$\forall a_i, a_j \in A$ 有 $a_i \circ a_j = a_i$. 则 A 中的每个元素都是$\circ$运算的右单位元，但没有左单位元，所以 A 中没有单位元. 同样地，A 中每个元素都是$\circ$运算的左零元，但没有零元.

关于单位元和零元存在以下定理.

定理 1.2　设$\circ$是集合 A 上的二元运算，若存在 $e_l \in A$ 和 $e_r \in A$ 满足 $\forall x \in A$ 有 $e_l \circ x = x$ 和 $x \circ e_r = x$，则 $e_l = e_r = e$，且 e 就是 A 中关于$\circ$运算的唯一的单位元.

证　因为 e_r 是右单位元，所以有 $e_l = e_l \circ e_r$，又由于 e_l 是左单位元，因此有 $e_l \circ e_r = e_r$. 由这两个等式可得 $e_l = e_r$，把这个单位元记作 e. 假设关于$\circ$运算存在另一个单位元 e'，则有

$$e' = e' \circ e = e,$$

所以 e 是关于$\circ$运算的唯一的单位元. ∎

定理 1.3　设$\circ$为集合 A 上的二元运算，若存在 $\theta_l \in A$ 和 $\theta_r \in A$ 使得 $\forall x \in A$ 有 $\theta_l \circ x = \theta_l$ 和 $x \circ \theta_r = \theta_r$，则 $\theta_l = \theta_r = \theta$，且 θ 是 A 中关于$\circ$运算的唯一的零元.

证明留作练习.

定理 1.4　设集合 A 至少含有两个元素，e 和 θ 分别为 A 中关于 $\circ$ 运算的单位元和零元，则 $e \neq \theta$.

证　假设 $e = \theta$，则 $\forall x \in A$ 有

$$x = x \circ e = x \circ \theta = \theta,$$

与 A 中至少含有两个元素矛盾. ∎

定义 1.7　设 $\circ$ 是集合 A 上的二元运算，$e \in A$ 是关于 $\circ$ 运算的单位元. 对于 $x \in A$ 若存在 $y_l \in A$(或 $y_r \in A$) 使得 $y_l \circ x = e$(或 $x \circ y_r = e$) 则称 y_l(或 y_r) 是 x 关于 $\circ$ 运算的**左(或右) 逆元**. 若 $y \in A$ 既是 x 关于 $\circ$ 运算的左逆元，又是 x 关于 $\circ$ 运算的右逆元，则称 y 是 x 关于 $\circ$ 运算的**逆元**.

【例 1.7】

(1) 在整数集 Z 中，任何整数 n 关于加法的逆元是 $-n$. 关于乘法只有 1 和 -1 存在逆元，就是它们自己，其它整数没有乘法逆元.

(2) n 阶($n \geqslant 2$) 实矩阵集合 $M_n(R)$ 中任何矩阵 M 的加法逆元为 $-M$. 而对于矩阵乘法只有实可逆矩阵 M 存在乘法逆元 M^{-1}.

(3) 幂集 $P(B)$ 中关于并运算只有空集 $\varnothing$ 有逆元，就是 $\varnothing$ 本身，B 的其它子集没有逆元.

关于逆元存在以下定理.

定理 1.5　设 $\circ$ 为集合 A 上可结合的二元运算且单位元为 e. 对于 $x \in A$ 若存在 y_l 和 $y_r \in A$ 使得 $y_l \circ x = e$ 和 $x \circ y_r = e$，则 $y_l = y_r = y$，且 y 是 x 关于 $\circ$ 运算的唯一的逆元.

证　$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r$.

令 $y = y_l = y_r$，则 y 是 x 关于 $\circ$ 运算的逆元.

假设 y' 也是 x 关于 $\circ$ 运算的逆元，则有

$$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y.$$

所以 y 是 x 关于 $\circ$ 运算的唯一的逆元. ∎

根据这个定理，对于任意 $x \in A$，如果存在关于二元运算的逆

元，则是唯一的. 可将这个唯一的逆元记作 x^{-1}.

【例1.8】 设$\circ$为实数集R上的二元运算，$\forall x \in R$ 有 $x \circ y = x + y - 2xy$，说明$\circ$运算是否为可交换的、可结合的、幂等的，然后确定关于$\circ$运算的单位元，零元和所有可逆元素的逆元.

解 $\circ$运算是可交换的、可结合的，但不是幂等的.

假设 e 和 θ 分别为$\circ$运算的单位元和零元，则 $\forall x \in R$ 有

$$x + e - 2xe = x \text{ 和 } x + \theta - 2x\theta = \theta,$$

即
$$(1 - 2x)e = 0 \text{ 和 } x(1 - 2\theta) = 0.$$

要使这些等式对一切实数 x 都成立，只有 $e = 0$ 和 $\theta = \frac{1}{2}$.

任取 $x \in R$，设 y 为 x 关于$\circ$运算的逆元，则有 $x + y - 2xy = 0$，从而解得 $y = \frac{-x}{1-2x}\ (x \neq \frac{1}{2})$.

通过上面的分析可知 0 是$\circ$运算的单位元，$\frac{1}{2}$ 是$\circ$运算的零元，$\forall x \in R(x \neq \frac{1}{2})$ 有 $x^{-1} = \frac{-x}{1-2x}$.

【例1.9】 设 A 上的二元运算$\circ$由表 1.3 所确定. 求 A 中关于$\circ$运算的单位元、零元和所有可逆元素的逆元.

表 1.3

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	d
c	c	a	a	d
d	d	d	d	d

解 由表 1.3 不难看出 a 是$\circ$运算的单位元，d 是$\circ$运算的零元. a,b,c 为可逆元素，且 $a^{-1} = a,\ b^{-1} = b,\ c^{-1} = c$.

下面给出关于二元运算的最后一条算律 —— 消去律.

定义 1.8 设$\circ$为集合 A 上的二元运算，若对于任意的 $a,b,c \in A$（a 不是$\circ$运算的零元）都有

$$a \circ b = a \circ c \Rightarrow b = c,$$
$$b \circ a = c \circ a \Rightarrow b = c.$$

则称$\circ$运算在 A 中适合消去律.

【例 1.10】

(1) 普通加法和乘法在整数集 Z,有理数集 Q,实数集 R 上适合消去律.

(2) n 阶($n \geqslant 2$) 实矩阵集合 $M_n(R)$ 上的矩阵加法适合消去律,但矩阵乘法不适合消去律.

(3) 幂集 $P(B)$ 上的并和交运算一般不适合消去律,但对称差运算适合消去律.

§1.2 代数系统、子代数和积代数

集合和集合上的运算可以构成代数系统.

定义 1.9 一个**代数系统**是一个三元组 $V = \langle A, \Omega, K\rangle$,其中 A 是一个非空的对象集合,称为 V 的**载体**;Ω 是一个非空的运算集合,即 $\Omega = \bigcup_{j=1}^{\infty} \Omega_j, \Omega_j = \{o \mid o$ 是 A 上的 j 元运算$\}$;$K \subseteq A$ 是**代数常数**的集合.

对于任何代数常数 $k \in K$,可以把 k 看成 A 上的**零元运算**,即 $k: \to A$. 这时可将代数系统 V 写作 $\langle A, \Omega\rangle$,其中 $\Omega = \bigcup_{j=0}^{\infty} \Omega_j, \Omega_0 = K$.

当 Ω 中含有 r 个代数运算时,r 为正整数,常常将 V 记作 $\langle A, o_1, o_2, \cdots, o_r\rangle$,其中 $o_1, o_2, \cdots, o_r$ 是代数运算,通常从高元运算到低元运算排列. 本书中如无特殊说明,所研究的代数系统就是这种含有有限个代数运算的系统. 例如 $\langle N, +, 0\rangle$, $\langle R, +, \cdot\rangle$, $\langle M_n(R), +, \cdot\rangle$, $\langle P(B), \cup, \cap, \varnothing\rangle$ 等都是这种代数系统. 在不产生误解的情况下,为了简便起见,可以不写出代数系统中所有的成分. 例如代数系统 $\langle N, +, 0\rangle$ 可以简记为 $\langle N, +\rangle$ 或 N.

【例 1.11】 图 1.1 是一个有穷半自动机,它的状态集 $Q = \{0,$

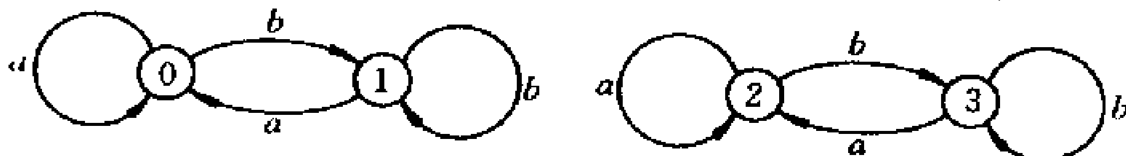


图 1.1

1,2,3},字母表 $\Sigma = \{a,b\}$,状态转移函数 $\sigma: Q \times \Sigma \to Q$ 如表 1.4 所示. 可以把这个有穷半自动机看作一个代数系统 $V = \langle Q, a, b \rangle$,其中 $Q = \{0,1,2,3\}$,a,b 是 Q 上的两个一元运算.
$a: Q \to Q, a(0) = a(1) = 0, a(2) = a(3) = 2.$
$b: Q \to Q, b(0) = b(1) = 1, b(2) = b(3) = 3.$

表 1.4

σ	a	b
0	0	1
1	0	1
2	2	3
3	2	3

【例1.12】 设 Σ 是有穷字母表,w 是 Σ 上的串,即 Σ 上的有限个字符构成的序列. 序列中的字符个数称为串的长度,记作 $|w|$. Λ 表示空串,$|\Lambda| = 0$. 对任意的 $k \in N$,令

$$\Sigma_k = \{a_{i_1} a_{i_2} \cdots a_{i_k} \mid a_{i_j} \in \Sigma\}$$

为 Σ 上所有长为 k 的串构成的集合,那么 $\Sigma_0 = \{\Lambda\}$. 定义 Σ^* 为 Σ 上所有串的集合,则

$$\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma_i,$$

$$\Sigma^+ = \Sigma^* - \{\Lambda\} = \bigcup_{i=1}^{\infty} \Sigma_i.$$

不难证明 Σ_k 为有穷集,Σ^* 和 Σ^+ 为可数集.

在 Σ^* 上定义二元运算$\circ$,$\forall w_1, w_2 \in \Sigma^*, w_1 = a_1 a_2 \cdots a_m$,$w_2 = b_1 b_2 \cdots b_n$ 有

$$w_1 \circ w_2 = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n,$$

称$\circ$为 Σ^* 上的连接运算.

$$\forall w \in \Sigma^*, w = a_1 a_2 \cdots a_m, \text{令 } w' = a_m a_{m-1} \cdots a_1,$$

则 $'$ 运算为 Σ^* 上的一元运算,称为求逆运算.

可以证明 Σ^* 上的连接运算满足结合律和消去律,单位元是空串 Λ. 称代数系统 $\langle \Sigma^*, \circ, ', \Lambda \rangle$ 为 Σ 上的**字代数**.

设 L 是 Σ^* 的子集,称 L 是 Σ 上的一个语言. 考虑幂集 $P(\Sigma^*)$,Σ 上所有语言的集合. 在 $P(\Sigma^*)$ 上定义二元运算 $\cup$,$\cap$ 和 $\cdot$,其中 $\cdot$ 运算是语言的连接运算. $\forall L_1, L_2 \in P(\Sigma^*)$ 有

$$L_1 \cdot L_2 = \{w_1 \circ w_2 \mid w_1 \in L_1 \text{ 且 } w_2 \in L_2\}.$$

不难证明并和交是可交换、可结合、幂等的，并且它们也是互相可分配的、可吸收的. 而语言连接运算 · 是可结合的，且 · 运算有单位元 $\Sigma_0 = \{\Lambda\}$. 在 $P(\Sigma^*)$ 上还可以定义一元运算 $\triangle$, $\forall L \in P(\Sigma^*)$ 有 $\triangle L = \{w' \mid w \in L\}$. $P(\Sigma^*)$ 和这些二元和一元运算构成了 Σ 上的**语言代数**.

下面考虑代数系统之间的关系.

定义 1.10 设 $V_1 = \langle A, o_1, o_2, \cdots, o_r\rangle$, $V_2 = \langle B, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r}\rangle$ 是具有 r 个运算的代数系统, $r \geqslant 1$. 若对于 $i = 1, 2, \cdots, r$, o_i 和 $\overline{o_i}$ 运算具有同样的元数，则称 V_1 和 V_2 是**同类型的代数系统**.

设 V_1, V_2, V_3 是代数系统. $V_1 = \langle R, +, \cdot, -, 0, 1\rangle$，其中 R 为实数集，$+$ 和 $\cdot$ 为普通的加法和乘法，$-$ 是求相反数运算. $V_2 = \langle M_n(R), +, \cdot, -, \theta, E\rangle$，其中 $M_n(R)$ 为 n 阶($n \geqslant 2$) 实矩阵集合，$+$ 和 $\cdot$ 分别为矩阵加法和乘法，对任意的 $M \in M_n(R)$, $M = (a_{ij})_{n\times n}$ 则 $-M = (-a_{ij})_{n\times n}$, θ 为 n 阶全 0 矩阵，E 为 n 阶单位矩阵. $V_3 = \langle P(B), \cup, \cap, \sim, \varnothing, B\rangle$，其中 $P(B)$ 为幂集，$\cup$ 和 $\cap$ 为集合的并和交，$\sim$ 为绝对补运算(全集为 B). 显然 V_1, V_2 和 V_3 都是同类型的代数系统，它们都有着共同的构成成分，但在运算性质方面却不一定相同. V_1 和 V_2 具有共同的运算性质：加法和乘法都适合交换律和结合律，乘法对加法适合分配律，$-$ 运算为求加法逆元的运算，0 和 θ 分别为加法的单位元，1 和 E 分别为乘法的单位元. 我们称 V_1 和 V_2 是**同种的代数系统**. 但它们和 V_3 不是同种的，因为 V_3 中的 $\cup$ 和 $\cap$ 运算互相适合分配律和吸收律，且一元运算 $\sim$ 不是关于 $\cup$ 运算的求逆运算. 对于代数结构这门课程来说，它并不是要研究每一个具体的代数系统，而是通过规定集合及集合上的二元、一元和零元运算以及运算所具有的性质来规范每一种代数系统. 这个代数系统是许多具有共同构成成分和运算性质的实际代数系统的模型或者抽象. 针对这个模型来研究它的结构和内在特征，然后运用到每个具体的代

数系统中去，这种研究方法就是抽象代数的基本方法. 后面涉及到的半群、独异点和群，环和域，格和布尔代数就是具有广泛应用背景的抽象的代数系统.

下面讨论子代数系统.

定义 1.11 设 $V = \langle A, o_1, o_2, \cdots, o_r \rangle$ 是代数系统，B 是 A 的非空子集，若 B 对 V 中所有的运算封闭，则称 $V' = \langle B, o_1, o_2, \cdots, o_r \rangle$ 是 V 的子代数系统，简称**子代数**. 当 B 是 A 的真子集时，称 V' 是 V 的**真子代数**.

【例 1.13】

(1) $\langle N, + \rangle$ 是 $\langle N, + \rangle$，$\langle Z, + \rangle$，$\langle Q, + \rangle$，$\langle R, + \rangle$ 的子代数. $\langle Z, +, 0 \rangle$ 是 $\langle R, +, 0 \rangle$，$\langle C, +, 0 \rangle$ 的真子代数.

(2) $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in R \right\}$，则 $\langle A, \cdot \rangle$ 是 $\langle M_2(R), \cdot \rangle$ 的真子代数，其中 $\cdot$ 为矩阵乘法. $M_2(R)$ 中关于 $\cdot$ 运算的单位元是 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$，若把乘法单位元看作 $M_2(R)$ 中的零元运算，那么 $\left\langle A, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\rangle$ 不是 $\left\langle M_2(R), \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ 的子代数，因为 A 对 $\left\langle M_2(R), \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ 中的零元运算不封闭.

定义 1.12 设 $V = \langle A, o_1, o_2, \cdots, o_r \rangle$ 是代数系统，其中零元运算的集合是 $K \subseteq A$. 若 K 对 V 中所有的运算封闭，则 $\langle K, o_1, o_2, \cdots, o_r \rangle$ 是 V 的子代数，称这个子代数和 V 自身是 V 的**平凡子代数**.

【例 1.14】 令 $nZ = \{nk \mid k \in Z\}$，$n \in N$，则 $\langle nZ, +, 0 \rangle$ 是 $\langle Z, +, 0 \rangle$ 的子代数. 因为 $\forall nk_1, nk_2 \in nZ$ 有

$$nk_1 + nk_2 = n(k_1 + k_2) \in nZ,$$

且 $0 \in nZ$，所以 nZ 对 $\langle Z, +, 0 \rangle$ 的运算都是封闭的.

当 $n = 0$ 时，$nZ = \{0\}$，$\langle \{0\}, +, 0 \rangle$ 是 $\langle Z, +, 0 \rangle$ 的平凡的真子代数. 当 $n = 1$ 时，$nZ = Z$，$\langle Z, +, 0 \rangle$ 也是平凡的子代数. 当 $n \neq 0, 1$ 时，$\langle nZ, +, 0 \rangle$ 是 $\langle Z, +, 0 \rangle$ 的非平凡的真子代数.

不难证明当代数系统 V 中只含有二元、一元和零元运算时，V 中二元运算的性质，如交换律、结合律、幂等律、消去律、分配律、吸收律等在 V 的子代数中都成立．当我们用这些性质和代数常数来定义代数系统时，V 的子代数和 V 不仅是同类型的，也是同种的代数系统．

设 V_1 和 V_2 是同类型的代数系统．由 V_1 和 V_2 可以构成一个新的代数系统 —— 积代数．

定义 1.13 设 $V_1 = \langle A, o_{11}, o_{12}, \cdots, o_{1r}\rangle, V_2 = \langle B, o_{21}, o_{22}, \cdots, o_{2r}\rangle$ 是同类型的代数系统，且对于 $i = 1,2,\cdots,r, o_{1i}$ 和 o_{2i} 是 k_i 元运算．V_1 和 V_2 的**积代数**记作 $V_1 \times V_2 = \langle A \times B, o_1, o_2, \cdots, o_r\rangle$，其中 o_i $(i = 1,2,\cdots,r)$ 是 k_i 元运算．对于任意的 $\langle x_1, y_2\rangle, \langle x_2, y_2\rangle, \cdots, \langle x_{k_i}, y_{k_i}\rangle \in A \times B$ 有

$$
\begin{aligned}
& o_i(\langle x_1, y_1\rangle, \langle x_2, y_2\rangle, \cdots, \langle x_{k_i}, y_{k_i}\rangle) \\
&= \langle o_{1i}(x_1, x_2, \cdots, x_{k_i}), o_{2i}(y_1, y_2, \cdots, y_{k_i})\rangle.
\end{aligned}
$$

若 V 是 V_1 与 V_2 的积代数，这时也称 V_1 和 V_2 是 V 的**因子代数**．显然积代数和它的因子代数是同类型的代数系统．

【例 1.15】 设 $V_1 = \langle R, +, \cdot\rangle$，其中 R 为实数集，$+, \cdot$ 分别为普通加法与乘法．$V_2 = \langle M_2(R), +, \cdot\rangle$，其中 $+, \cdot$ 为矩阵加法和乘法，则 $V_1 \times V_2 = \langle R \times M_2(R), \oplus, \odot\rangle$，对于 $\left\langle 3, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\rangle$，$\left\langle 4, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\rangle \in R \times M_2(R)$ 有

$$
\left\langle 3, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\rangle \oplus \left\langle 4, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\rangle = \left\langle 7, \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}\right\rangle,
$$

$$
\left\langle 3, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\rangle \odot \left\langle 4, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\rangle = \left\langle 12, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\rangle.
$$

关于积代数有以下定理．

定理 1.6 设代数系统 $V_1 = \langle A, o_{11}, o_{12}, \cdots, o_{1r}\rangle, V_2 = \langle B, o_{21}, o_{22}, \cdots, o_{2r}\rangle$ 是同类型的，V 是 V_1 与 V_2 的积代数．对任意的二元运算 $o_{1i}, o_{1j}, o_{2i}, o_{2j}$，

(1) 若 o_{1i}, o_{2i} 在 V_1 和 V_2 中是可交换的(或可结合的,幂等的),则 o_i 在 V 中也是可交换的(或可结合的,幂等的).

(2) 若 o_{1i} 对 o_{1j} 在 V_1 上是可分配的,o_{2i} 对 o_{2j} 在 V_2 上是可分配的,则 o_i 对 o_j 在 V 上也是可分配的.

(3) 若 o_{1i}, o_{1j} 在 V_1 上是吸收的,且 o_{2i}, o_{2j} 在 V_2 上也是吸收的,则 o_i, o_j 在 V 上是吸收的.

(4) 若 e_1(或 θ_1) 为 V_1 中关于 o_{1i} 运算的单位元(或零元),e_2(或 θ_2) 为 V_2 中关于 o_{2i} 运算的单位元(或零元),则 $\langle e_1, e_2\rangle$(或 $\langle\theta_1, \theta_2\rangle$) 为 V 中关于 o_i 运算的单位元(或零元).

(5) 若 o_{1i}, o_{2i} 为含有单位元的二元运算,且 $a \in A, b \in B$ 关于 o_{1i} 和 o_{2i} 运算的逆元分别为 a^{-1}, b^{-1},则 $\langle a^{-1}, b^{-1}\rangle$ 是 $\langle a, b\rangle$ 在 V 中关于 o_i 运算的逆元.

证 这里只给出关于(1) 中的交换律和(4) 的单位元的证明,其余留作练习.

(1) 任取 $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in A \times B$,

$$\langle a_1, b_1\rangle o_i \langle a_2, b_2\rangle = \langle a_1 o_{1i} a_2,\ b_1 o_{2i} b_2\rangle$$

$$= \langle a_2 o_{1i} a_1,\ b_2 o_{2i} b_1\rangle = \langle a_2, b_2\rangle o_i \langle a_1, b_1\rangle.$$

(4) 任取 $\langle a, b\rangle \in A \times B$,

$$\langle a, b\rangle o_i \langle e_1, e_2\rangle = \langle a o_{1i} e_1,\ b o_{2i} e_2\rangle = \langle a, b\rangle,$$

$$\langle e_1, e_2\rangle o_i \langle a, b\rangle = \langle e_1 o_{1i} a,\ e_2 o_{2i} b\rangle = \langle a, b\rangle.$$ ∎

由定理 1.6 可以知道积代数和它的因子代数在许多性质上是一致的,但消去律是一个例外. 有时 V_1 和 V_2 都满足消去律,但 $V_1 \times V_2$ 却不满足消去律. 请看下面的例子.

【例 1.16】 $V_1 = \langle Z_2, \otimes_2\rangle, V_2 = \langle Z_3, \otimes_3\rangle$,其中 $Z_2 = \{0,1\}$,$Z_3 = \{0,1,2\}$,$\otimes_2$ 和 $\otimes_3$ 分别为模 2 乘法和模 3 乘法. V_1 和 V_2 的积代数为 $\langle Z_2 \times Z_3, \otimes\rangle$. 对于任意的 $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle \in Z_2 \times Z_3$ 有

$$\langle x_1, y_1\rangle \otimes \langle x_2, y_2\rangle = \langle x_1 \otimes_2 x_2, y_1 \otimes_3 y_2\rangle.$$

假设 $\otimes$ 运算满足消去律,必有

$$\langle 0,1\rangle \otimes \langle 1,0\rangle = \langle 0,1\rangle \otimes \langle 0,0\rangle \Rightarrow \langle 1,0\rangle = \langle 0,0\rangle.$$

这显然是不对的，因此 $\otimes$ 运算不满足消去律.

可以把两个代数系统的积代数的概念推广到 n 个代数系统.

定义 1.14 设 $V_1, V_2, \cdots, V_n$ 是同类型的代数系统. 对于 $i = 1, 2, \cdots, n$, $V_i = \langle A_i, o_{i1}, o_{i2}, \cdots, o_{ir}\rangle$. 设 o_{it} 为 k_t 元运算, $t = 1, 2, \cdots r$. $V_1, V_2, \cdots, V_n$ 的积代数记为

$$V_1 \times V_2 \times \cdots \times V_n = \langle A_1 \times A_2 \times \cdots \times A_n, o_1, o_2, \cdots, o_r\rangle.$$

其中 o_t 是 k_t 元运算, $t = 1, 2 \cdots, r$. 对于任意的 $\langle x_{1j}, x_{2j}, \cdots, x_{nj}\rangle \in A_1 \times A_2 \times \cdots \times A_n$, $j = 1, 2, \cdots, k_t$ 有

$$o_t(\langle x_{11}, x_{21}, \cdots, x_{n1}\rangle, \langle x_{12}, x_{22}, \cdots, x_{n2}\rangle, \cdots, \langle x_{1k_t}, x_{2k_t}, \cdots, x_{nk_t}\rangle)$$

$$= \langle o_{1t}(x_{11}, x_{12}, \cdots, x_{1k_t}),\ o_{2t}(x_{21}, x_{22}, \cdots, x_{2k_t}), o_{nt}(x_{n1}, x_{n2}, \cdots, x_{nk_t})\rangle.$$

【例1.17】 设 $V = \langle N, +\rangle$, 则 $V \times V \times V = \langle N \times N \times N, \oplus\rangle$, 对于任意的 $\langle a_1, a_2, a_3\rangle, \langle b_1, b_2, b_3\rangle \in N \times N \times N$ 有

$$\langle a_1, a_2, a_3\rangle \oplus \langle b_1, b_2, b_3\rangle = \langle a_1 + b_1,\ a_2 + b_2,\ a_3 + b_3\rangle.$$

可以证明定理 1.6 的结论对于 n 个代数系统的积代数也成立.

§1.3 代数系统的同态与同构

同态映射是研究代数系统之间相互关系的重要工具，我们先给出同态映射的定义.

定义 1.15 设 $V_1 = \langle A, o_1, o_2, \cdots, o_r\rangle$, $V_2 = \langle B, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r}\rangle$ 是同类型的代数系统. 对于 $i = 1, 2, \cdots, r$, o_i 和 $\overline{o_i}$ 是 k_i 元运算. 函数 $\varphi: A \to B$, 如果对所有的运算 $o_i, \overline{o_i}$ 都有

$$\varphi(o_i(x_1, x_2, \cdots, x_{k_i})) = \overline{o_i}(\varphi(x_1), \varphi(x_2), \cdots, \varphi(x_{k_i})),$$

$$\forall x_1, x_2, \cdots, x_{k_i} \in A,$$

则称 φ 是代数系统 V_1 到 V_2 的**同态映射**，简称同态.

对于二元运算 $\circ, \bar{\circ}$, 一元 $\triangle, \bar{\triangle}$ 和零元运算 $a, \bar{a}$, 上述定义中的等式可分别表示为：

$$\varphi(x \circ y) = \varphi(x) \bar{\circ} \varphi(y), \quad \forall x, y \in A,$$
$$\varphi(\triangle x) = \bar{\triangle} \varphi(x), \quad \forall x \in A,$$
$$\varphi(a) = \bar{a}.$$

【例 1.18】 设代数系统 $V_1 = \langle Z, + \rangle, V_2 = \langle Z_n, \oplus \rangle$，其中 $Z_n = \{0,1,\cdots,n-1\}$，$\oplus$ 为模 n 加法. 定义 $\varphi: Z \to Z_n, \varphi(x) = (x)\bmod n$，则 φ 为 V_1 到 V_2 的同态. 因为对任意的 $x, y \in Z$ 有

$$\begin{aligned}\varphi(x+y) &= (x+y)\bmod n = (x)\bmod n \oplus (y)\bmod n \\ &= \varphi(x) \oplus \varphi(y).\end{aligned}$$

定义 1.16 设 $V_1 = \langle A, o_1, o_2, \cdots, o_r \rangle, V_2 = \langle B, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r} \rangle$ 是同类型的代数系统，$\varphi: A \to B$ 是 V_1 到 V_2 的同态.

(1) 若 $\varphi: A \to B$ 是满射的，则称 φ 是**满同态**，记为 $V_1 \overset{\varphi}{\sim} V_2$.

(2) 若 $\varphi: A \to B$ 是单射的，则称 φ 是**单同态**.

(3) 若 $\varphi: A \to B$ 是是双射的，则称 φ 是**同构**，记为 $V_1 \overset{\varphi}{\cong} V_2$，这时也称 V_1 同构于 V_2.

(4) 若 $V_1 = V_2$，则称 φ 是**自同态**. 若 φ 又是双射的则称 φ 是**自同构**.

如果代数系统 V_1 同构于 V_2，从抽象代数的观点看，它们是没有区别的，是同一个代数系统.

【例 1.19】 $V = \langle Z, + \rangle$，$+$ 为普通加法，$c \in Z$. 定义 $\varphi_c: Z \to Z, \varphi_c(x) = cx, \forall x \in A$. 则 $\forall x, y \in Z$ 有

$$\varphi_c(x+y) = c(x+y) = cx + cy = \varphi_c(x) + \varphi_c(y).$$

φ_c 是 V 上的自同态.

当 $c = 0$ 时，$\forall x \in Z$ 有 $\varphi_0(x) = 0$，称 φ_0 是**零同态**. 它不是单同态也不是满同态.

当 $c = \pm 1$ 时，有 $\varphi_1(x) = x, \varphi_{-1}(x) = -x, \forall x \in Z$. φ_1 和 φ_{-1} 是 V 上的两个自同构.

当 $c \neq \pm 1, 0$ 时，$\forall x \in Z$ 有 $\varphi_c(x) = cx$，φ_c 是 V 上的**单自同态**.

【例 1.20】 设 Σ 为有限字母表，Σ^* 为 Σ 上有限长度的串的集

合，$\Lambda \in \Sigma^*$ 为空串，Σ^* 和串的连接运算构成代数系统$\langle \Sigma^*, \circ, \Lambda \rangle$. 令 $\varphi: \Sigma^* \to N, \varphi(w) = |w|, \forall w \in \Sigma^*$. 则 $\forall w_1, w_2 \in \Sigma^*$ 有

$$\varphi(w_1 \circ w_2) = |w_1 \circ w_2| = |w_1| + |w_2| = \varphi(w_1) + \varphi(w_2),$$

且有 $\varphi(\Lambda) = 0$，所以 φ 是$\langle \Sigma^*, \circ, \Lambda \rangle$到$\langle N, +, 0 \rangle$的同态，且为满同态. 当 Σ 中只含一个字母时，φ 为同构.

下面讨论同态的性质.

定理 1.7　设 $V_1 = \langle A, o_1, o_2, \cdots, o_r \rangle, V_2 = \langle B, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r} \rangle$ 是同类型的代数系统，对于 $i = 1, 2, \cdots, r, o_i, \overline{o_i}$ 是 k_i 元运算. $\varphi: A \to B$ 是 V_1 到 V_2 的同态，则 $\varphi(A)$ 关于 V_2 中的运算构成代数系统，且是 V_2 的子代数，称为 V_1 在 φ 下的**同态像**.

证　$\varphi(A) \subseteq B$，且 $\varphi(A) \neq \varnothing$. 只须证明 $\varphi(A)$ 对 V_2 中所有的运算封闭即可. 若 V_2 中存在零元运算 $\overline{a}$，则 V_1 中存在对应的零元运算 a，且 $\varphi(a) = \overline{a}$. 所以 $\overline{a} \in \varphi(A)$. 下面考虑 V_2 中的非零元运算$\overline{o_i}$. 对于 $\varphi(A)$ 中的任意 k_i 个元素 $y_1, y_2, \cdots y_{k_i}$，存在 $x_1, x_2, \cdots, x_{k_i} \in A$ 使得 $\varphi(x_j) = y_j, j = 1, 2, \cdots, k_i$. 因此有

$$\begin{aligned}\overline{o_i}(y_1, y_2, \cdots, y_{k_i}) &= \overline{o_i}(\varphi(x_1), \varphi(x_2), \cdots, \varphi(x_{k_i})) \\ &= \varphi(o_i(x_1, x_2, \cdots, x_{k_i})) \in \varphi(A).\end{aligned}$$

这就证明了$\langle \varphi(A), \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r} \rangle$ 是 V_2 的子代数. ∎

【例 1.21】　设 $V_1 = \langle R, +, 0 \rangle, V_2 = \langle R^*, \cdot, 1 \rangle$，其中 R 为实数集，$R^* = R - \{0\}$，$+$ 和 $\cdot$ 分别为普通加法和乘法. 令 $\varphi: R \to R^*$，$\varphi(x) = e^x, \forall x \in R$，则不难证明 φ 为 V_1 到 V_2 的同态. V_1 在 φ 下的同态像为$\langle R^+, \cdot, 1 \rangle$，是$\langle R^*, \cdot, 1 \rangle$ 的子代数.

定理 1.8　设 $V_1 = \langle A, o_1, o_2, \cdots, o_r \rangle, V_2 = \langle B, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r} \rangle$ 是同类型的代数系统，$\varphi: A \to B$ 是 V_1 到 V_2 的满同态，o_i, o_j 是 V_1 中的两个二元运算.

(1) 若 o_i 是可交换的(或可结合的，幂等的)，则$\overline{o_i}$ 也是可交换的(或可结合的，幂等的).

(2) 若 o_i 对 o_j 是可分配的，则$\overline{o_i}$ 对$\overline{o_j}$ 也是可分配的.

(3) 若 o_i，o_j 是可吸收的，则$\overline{o_i}$，$\overline{o_j}$ 也是可吸收的.

(4) 若 e(或 θ) 是 V_1 中关于 o_i 运算的单位元(或零元)，则 $\varphi(e)$(或 $\varphi(\theta)$) 是 V_2 中关于$\overline{o_i}$ 运算的单位元(或零元).

(5) 若 o_i 是含有单位元的运算，$x^{-1} \in A$ 是 x 关于 o_i 运算的逆元，则 $\varphi(x^{-1})$ 是 $\varphi(x)$ 关于$\overline{o_i}$ 运算的逆元.

证 这里只给出(1) 中的结合律和(5) 的证明，其它留作练习.

(1) 任取 $x,y,z \in B$，因 φ 是满同态，所以存在 $a,b,c \in A$ 使得

$$\varphi(a) = x, \varphi(b) = y, \varphi(c) = z.$$

$$\begin{aligned}(x\,\overline{o_i}y)\,\overline{o_i}z &= (\varphi(a)\,\overline{o_i}\varphi(b))\,\overline{o_i}\varphi(c) = \varphi(ao_ib)\,\overline{o_i}\varphi(c)\\ &=\varphi((ao_ib)o_ic) = \varphi(ao_i(bo_ic)) = \varphi(a)\,\overline{o_i}\varphi(bo_ic)\\ &=\varphi(a)\,\overline{o_i}(\varphi(b)\,\overline{o_i}\varphi(c)) = x\,\overline{o_i}(y\,\overline{o_i}z).\end{aligned}$$

(5) $\varphi(x)\,\overline{o_i}\varphi(x^{-1}) = \varphi(xo_ix^{-1}) = \varphi(e)$.

$$\varphi(x^{-1})\,\overline{o_i}\varphi(x) = \varphi(x^{-1}o_ix) = \varphi(e).$$

由逆元的唯一性知 $\varphi(x^{-1})$ 是 $\varphi(x)$ 的逆元. ∎

定理 1.8 中 φ 为满同态的条件很重要，当 φ 不是满同态时定理的结论仅在 V_1 的同态像$\langle\varphi(A),\overline{o_1},\overline{o_2},\cdots,\overline{o_r}\rangle$ 中成立. 请看下面两个例子.

【例 1.22】 设代数系统 $V_1 = \langle A, * \rangle$，$V_2 = \langle B,\circ\rangle$，其中 $A = \{a,b,c,d\}$，$B = \{0,1,2,3\}$. $*$ 和$\circ$运算由运算表(见表1.5)给定. 定义函数 φ: $A \to B$，$\varphi(a) = 0$，$\varphi(b) = 1$，$\varphi(c) = 0$，$\varphi(d) = 1$. 可以验证 φ 是 V_1 到 V_2 的同态. V_1 在 φ 下的同态像是$\langle\{0,1\},\circ\rangle$. 不难证明 V_1 中的 $*$ 运算满足结合律，但 V_2 中的$\circ$运算却不满足结合律，因为有

表 1.5

$*$	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

$\circ$	0	1	2	3
0	0	1	1	0
1	1	1	2	1
2	1	2	3	2
3	0	1	2	3

$$(1\circ 0)\circ 2 = 1\circ 2 = 2 \quad 和 \quad 1\circ(0\circ 2) = 1\circ 1 = 1.$$

【例 1.23】 设代数系统 $V = \langle A, \cdot\rangle$，其中 $A = \left\{\begin{pmatrix} a & 0 \\ 0 & d\end{pmatrix} \middle| a, d \in R\right\}$，$\cdot$ 为矩阵乘法. 定义函数 $\varphi: A \to A, \varphi\left(\begin{pmatrix} a & 0 \\ 0 & d\end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & 0\end{pmatrix}$，$\forall \begin{pmatrix} a & 0 \\ 0 & d\end{pmatrix} \in A$. φ 是 V 上的自同态，但不是满自同态. 因为任取 $\begin{pmatrix} a_1 & 0 \\ 0 & d_1\end{pmatrix}, \begin{pmatrix} a_2 & 0 \\ 0 & d_2\end{pmatrix} \in A$ 有

$$\varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & d_1\end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ 0 & d_2\end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a_1a_2 & 0 \\ 0 & d_1d_2\end{pmatrix}\right) = \begin{pmatrix} a_1a_2 & 0 \\ 0 & 0\end{pmatrix},$$

$$\varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & d_1\end{pmatrix}\right) \cdot \varphi\left(\begin{pmatrix} a_2 & 0 \\ 0 & d_2\end{pmatrix}\right) = \begin{pmatrix} a_1 & 0 \\ 0 & 0\end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ 0 & 0\end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ 0 & 0\end{pmatrix}.$$

所以 $$\varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & d_1\end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ 0 & d_2\end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & d_1\end{pmatrix}\right) \cdot \varphi\left(\begin{pmatrix} a_2 & 0 \\ 0 & d_2\end{pmatrix}\right).$$

V 在 φ 下的同态像是 $\langle B, \cdot\rangle$，其中 $B = \left\{\begin{pmatrix} a & 0 \\ 0 & 0\end{pmatrix} \middle| a \in R\right\}$. 考虑 V 中关于 $\cdot$ 运算的单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$，$\varphi$ 将它映到 $\begin{pmatrix} 1 & 0 \\ 0 & 0\end{pmatrix}$，但 $\begin{pmatrix} 1 & 0 \\ 0 & 0\end{pmatrix}$ 不是 V 中的单位元，而是同态像 $\langle B, \cdot\rangle$ 中的单位元.

对于这个定理我们还要再说明一点. 同态映射可以保持代数系统 V_1 中的许多性质，如交换律、结合律、幂等律、分配律、吸收律等，但对消去律不一定为真. 请看下面的例子.

【例 1.24】 $V_1 = \langle Z, \cdot\rangle, V_2 = \langle Z_6, \otimes\rangle$ 为代数系统，其中 $Z_6 = \{0,1,\cdots,5\}$，$\otimes$ 为模 6 乘法. 令 $\varphi: Z \to Z_6$. $\varphi(x) = (x)\bmod 6, \forall x \in Z$，则 φ 为 V_1 到 V_2 的满同态. 不难看到，普通乘法 $\cdot$ 在 Z 上是满足消去律的，而模 6 乘法 $\otimes$ 在 Z_6 上不满足消去律. 考虑等式 $2 \otimes 3 = 2 \otimes 0$，若成立消去律就得到 $2 = 0$，显然是不对的.

【例 1.25】 设代数系统 $V = \langle Z_n, \oplus, 0\rangle$，其中 $Z_n = \{0,1,\cdots, n-1\}$，$\oplus$ 为模 n 加法. 证明 V 上恰好存在着 n 个自同态.

证 首先证明 V 上存在着 n 个自同态. 考虑 $\varphi_p: Z_n \to Z_n, \varphi_p(x)$

$= (px)\bmod n$, $\forall x \in Z_n$，其中 $p = 0,1,\cdots,n-1$. 易证 φ_p 是 V 上的自同态. 任取 $x,y \in Z_n$，有

$$\varphi_p(x \oplus y) = (p(x \oplus y))\bmod n$$
$$= (px)\bmod n \oplus (py)\bmod n = \varphi_p(x) \oplus \varphi_p(y),$$
$$\varphi_p(0) = (p0)\bmod n = (0)\bmod n = 0.$$

下面证明 V 上的任何自同态必为上述 n 个自同态之一. 设 $\varphi: Z_n \to Z_n$ 是 V 上的自同态，所以有 $\varphi(0) = 0$. 假设 $\varphi(1) = i, i \in Z_n$，我们将要证明 $\forall x \in Z_n$，有 $\varphi(x) = (ix)\bmod n$.

若 $x = 0$，则 $\varphi(0) = 0 = (i0)\bmod n$.

假若对任意的 $j \in \{0,1,\cdots,n-2\}$ 有 $\varphi(j) = (ij)\bmod n$，则

$$\varphi(j+1) = \varphi(j \oplus 1) = \varphi(j) \oplus \varphi(1) = (ij)\bmod n \oplus i$$
$$= (i(j+1))\bmod n.$$

所以 $\forall x \in Z_n$ 有 $\varphi(x) = (ix)\bmod n$. ∎

§1.4　同余关系和商代数

定义 1.17　设代数系统 $V = \langle A, o_1, o_2, \cdots, o_r \rangle$，其中 o_i 为 k_i 元运算. 关系 $\sim$ 是 A 上的等价关系. 任取 A 上 $2k_i$ 个元素 $a_1, a_2, \cdots, a_{k_i}, b_1, b_2, \cdots, b_{k_i}$，如果对 $j = 1,2,\cdots,k_i$，$a_j \sim b_j$ 成立就有

$$o_i(a_1,a_2,\cdots,a_{k_i}) \sim o_i(b_1,b_2,\cdots,b_{k_i}),$$

则称等价关系 $\sim$ 对运算 o_i 具有**置换性质**. 如果等价关系 $\sim$ 对 V 中所有的运算都具有置换性质，则称关系 $\sim$ 是 V 上的**同余关系**，称 A 中关于 $\sim$ 的等价类为 V 上的**同余类**.

由于零元运算与运算数无关，所以 A 上的等价关系对所有零元运算都具有置换性质. 为判断 A 上的等价关系是否为同余关系，只须验证该关系对 V 上每一个非零元运算是否具有置换性质即可.

【例 1.26】　设代数系统 $V = \langle A, \cdot, -, \triangle \rangle$，其中 $A = \left\{\frac{a}{b} \middle| a,b \in R \wedge b \neq 0\right\}$，$\cdot$ 为普通乘法，$-$ 为求相反数，且 $\forall \frac{a}{b} \in A$

有$\triangle\frac{a}{b}=\frac{a}{b^2}$. 在$A$上定义等价关系$\sim$,$\forall\frac{a}{b},\frac{c}{d}\in A$,$\frac{a}{b}\sim\frac{c}{d}\Leftrightarrow ad=bc$. 下面检查关系$\sim$对$V$中运算是否具有置换性质. 任取$\frac{a}{b},\frac{c}{d},\frac{e}{f},\frac{g}{h}\in A$,有

$$\frac{a}{b}\sim\frac{c}{d}\wedge\frac{e}{f}\sim\frac{g}{h}\Rightarrow ad=bc\wedge eh=fg\Rightarrow aedh=bfcg$$

$$\Rightarrow\frac{ae}{bf}\sim\frac{cg}{dh}\Rightarrow\frac{a}{b}\cdot\frac{e}{f}\sim\frac{c}{d}\cdot\frac{g}{h}.$$

$$\frac{a}{b}\sim\frac{c}{d}\Rightarrow ad=bc\Rightarrow -ad=-bc\Rightarrow-\frac{a}{b}\sim-\frac{c}{d}.$$

所以关系$\sim$对于$\cdot$和$-$运算具有置换性质,而对$\triangle$运算不具有置换性质. 例如$\frac{1}{2}\sim\frac{2}{4}$,但$\triangle\frac{1}{2}=\frac{1}{4}$,$\triangle\frac{2}{4}=\frac{2}{16}$,$\frac{1}{4}\not\sim\frac{2}{16}$.

由代数系统V和V上的同余关系可以构造出新的代数系统——商代数.

定义1.18 设代数系统$V=\langle A,o_1,o_2,\cdots,o_r\rangle$,其中$o_i$为$k_i$元运算. 关系$\sim$是$V$上的同余关系,$V$关于同余关系$\sim$的商代数记作$V/\sim=\langle A/\sim,\overline{o_1},\overline{o_2},\cdots,\overline{o_r}\rangle$,其中$A/\sim$是$A$关于同余关系$\sim$的商集. 对于$i=1,2,\cdots,r$,运算$\overline{o_i}$规定为:$\forall[a_1],[a_2],\cdots,[a_{k_i}]\in A/\sim$,有

$$\overline{o_i}([a_1],[a_2],\cdots,[a_{k_i}])=[o_i(a_1,a_2,\cdots,a_{k_i})].$$

为了说明商代数$V/\sim$是有意义的,必须证明$V/\sim$中的所有运算都是良定义的,即证明运算结果与同余类的代表元素的选取无关. 对于$i=1,2,\cdots,r$,考虑$V/\sim$中的运算$\overline{o_i}$. 任取k_i个同余类$[a_1],[a_2],\cdots,[a_{k_i}]$. 假设$A$中存在$b_1,b_2,\cdots,b_{k_i}$,使得$b_j\in[a_j]$, $j=1,2,\cdots,k_i$,我们只须证明

$$\overline{o_i}([a_1],[a_2],\cdots,[a_{k_i}])=\overline{o_i}([b_1],[b_2],\cdots,[b_{k_i}]).$$

对于任意$j=1,2,\cdots,k_i$,由$b_j\in[a_j]$可知$a_j\sim b_j$. 关系$\sim$是V上同余关系,所以$\sim$关于o_i运算具有置换性质,即$o_i(a_1,a_2,\cdots,a_{k_i})\sim$

$o_i(b_1,b_2,\cdots,b_{k_i})$. 因此有$[o_i(a_1,a_2,\cdots,a_{k_i})]=[o_i(b_1,b_2,\cdots,b_{k_i})]$. 根据商代数的定义，有$\overline{o_i}([a_1],[a_2],\cdots,[a_{k_i}])=\overline{o_i}([b_1],[b_2],\cdots,[b_{k_i}])$.

【例 1.27】 设$V=\langle Z,\cdot\rangle$,其中·为普通乘法,如下定义Z上的等价关系$\sim$:$\forall x,y\in Z$有$x\sim y\Leftrightarrow x\equiv y(\mathrm{mod}4)$,则$\sim$为$V$上的同余关系.$V$关于$\sim$的商代数$V/\sim=\langle Z/\sim,\odot\rangle$,其中$Z/\sim=\{[0],[1],[2],[3]\}$. $\forall[x],[y]\in Z/\sim$有$[x]\odot[y]=[(x\cdot y)\mathrm{mod}4]$. 从同构的意义上说，商代数$V/\sim$就是代数系统$\langle Z_4,\otimes\rangle$,其中$Z_4=\{0,1,2,3\}$, $\otimes$为模4乘法.

由定义1.18可以看出代数系统V和商代数$V/\sim$是同类型的.进一步可以证明商代数$V/\sim$能够保持V中的许多运算性质.

定理 1.9 设$V=\langle A,o_1,o_2,\cdots,o_r\rangle$是代数系统,对于$i=1,2,\cdots,r$,$o_i$是$k_i$元运算. $\sim$是V上的同余关系,V关于$\sim$的商代数$V/\sim=\langle A/\sim,\overline{o_1},\overline{o_2},\cdots,\overline{o_r}\rangle$. 令$o_i,o_j$是$V$中任意的二元运算.

(1) 若o_i是可交换的(或可结合的,幂等的),则$\overline{o_i}$在$V/\sim$中也是可交换的(或可结合的,幂等的).

(2) 若o_i对o_j是可分配的,则$\overline{o_i}$对$\overline{o_j}$在$V/\sim$中也是可分配的.

(3) 若o_i,o_j满足吸收律,则$\overline{o_i},\overline{o_j}$在$V/\sim$中也满足吸收律.

(4) 若e(或θ)为V中关于o_i运算的单位元(或零元),则$[e]$(或$[\theta]$)是$V/\sim$中关于$\overline{o_i}$运算的单位元(或零元).

(5) 若o_i为V中含单位元的运算,且$x\in A$关于o_i运算的逆元为x^{-1}.则在$V/\sim$中$[x]$关于$\overline{o_i}$运算的逆元是$[x^{-1}]$.

证明留作练习.

下面给出几个关于同态,同余关系和商代数的重要定理.

定理 1.10 设$V_1=\langle A,o_1,o_2,\cdots,o_r\rangle$,$V_2=\langle B,\overline{o_1},\overline{o_2},\cdots,\overline{o_r}\rangle$是同类型的代数系统.对于$i=1,2,\cdots,r$,$o_i$和$\overline{o_i}$是$k_i$元运算.令$\varphi:A\to B$是$V_1$到$V_2$的同态,则由$\varphi$导出的$A$上的等价关系$\sim$是$V_1$上的同余关系.

证 $\sim$ 是由 φ 导出的等价关系，所以 $\forall x,y \in A$ 有 $x \sim y \Leftrightarrow \varphi(x) = \varphi(y)$. 任取一个 V_1 上的运算 $o_i(k_i \geqslant 1)$，设 $a_1,a_2,\cdots,a_{k_i},b_1,b_2,\cdots,b_{k_i} \in A$，且 $a_j \sim b_j, j = 1,2,\cdots,k_i$，则有 $\varphi(a_j) = \varphi(b_j)$. 因此有下面的等式：

$$\overline{o_i}(\varphi(a_1),\varphi(a_2),\cdots,\varphi(a_{k_i})) = \overline{o_i}(\varphi(b_1),\varphi(b_2),\cdots,\varphi(b_{k_i})).$$

又由于 φ 是同态，所以得

$$\varphi(o_i(a_1,a_2,\cdots,a_{k_i})) = \varphi(o_i(b_1,b_2,\cdots,b_{k_i})).$$

从而有 $o_i(a_1,a_2,\cdots,a_{k_i}) \sim o_i(b_1,b_2,\cdots,b_{k_i})$. 这就证明了等价关系 $\sim$ 关于 o_i 运算有置换性质. 由于 i 的任意性可知 $\sim$ 是 V_1 上的同余关系. ∎

【例 1.28】 设代数系统 $V_1 = \langle \Sigma^*, \circ, \Lambda \rangle$，$V_2 = \langle N, +, 0 \rangle$，其中 Σ^* 为 Σ 上的串的集合，$\circ$ 为连接运算，Λ 为空串. 定义 $\varphi: \Sigma^* \to N$，$\varphi(w) = |w|, \forall w \in \Sigma^*$，则 φ 为 V_1 到 V_2 的同态映射. 由 φ 导出的 V_1 上的同余关系 $\sim$ 可定义为：$\forall w_1,w_2 \in \Sigma^*, w_1 \sim w_2 \Leftrightarrow |w_1| = |w_2|$，由这个同余关系确定的同余类恰为等长的串所组成.

定理 1.11 设 $V = \langle A,o_1,o_2,\cdots,o_r \rangle$ 是代数系统，其中 o_i 为 k_i 元运算，$i = 1,2,\cdots,r$. $\sim$ 为 V 上的同余关系，则**自然映射** $g: A \to A/\sim, g(a) = [a], \forall a \in A$ 是从 V 到 $V/\sim$ 上的同态映射.

证 设 V 关于同余关系 $\sim$ 的商代数是 $V/\sim = \langle A/\sim, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r} \rangle$. 对于 $i = 1,2,\cdots,r$，考虑 k_i 元运算 o_i，任取 $a_1,a_2,\cdots,a_{k_i} \in A$ 有

$$g(o_i(a_1,a_2,\cdots,a_{k_i})) = [o_i(a_1,a_2,\cdots,a_{k_i})]$$
$$= \overline{o_i}([a_1],[a_2],\cdots,[a_{k_i}]) = \overline{o_i}(g(a_1),g(a_2),\cdots,g(a_{k_i})).$$

所以 g 是 V 到 $V/\sim$ 的同态映射. ∎

定理 1.12 （同态基本定理）设 $V_1 = \langle A,o_1,o_2,\cdots,o_r \rangle$，$V_2 = \langle B,o'_1,o'_2,\cdots,o'_r \rangle$ 是同类型的代数系统，对于 $i = 1,2,\cdots,r$，o_i,o'_i 是 k_i 元运算，$\varphi: A \to B$ 是 V_1 到 V_2 的同态，关系 $\sim$ 是 φ 导出的 V_1 上的同余关系，则 V_1 关于同余关系 $\sim$ 的商代数同构于 V_1 在 φ 下的同态像，

即$V_1/\sim\ \cong \langle\varphi(A),o'_1,o'_2,\cdots,o'_r\rangle$.

证　设V_1关于同余关系$\sim$的商代数为

$$V_1/\sim\ =\langle A/\sim,\overline{o_1},\overline{o_2},\cdots,\overline{o_r}\rangle.$$

定义$h: A/\sim\ \rightarrow\varphi(A)$, $h([a])=\varphi(a)$, $\forall[a]\in A/\sim$,任取$a,b\in A$,有

$$[a]=[b]\Leftrightarrow a\sim b\Leftrightarrow\varphi(a)=\varphi(b)\Leftrightarrow h([a])=h([b]).$$

这就证明了h是单射的函数.再考虑h的满射性,$\forall y\in\varphi(A)$,存在$x\in A$使$\varphi(x)=y$,因此有$[x]\in A/\sim$,满足$h([x])=\varphi(x)=y$,从而h是双射的.最后证明h为同态映射.对于$i=1,2,\cdots,r$,取商代数$V_1/\sim$中的k_i元运算$\overline{o_i}$,$\forall[a_1],[a_2],\cdots,[a_{k_i}]\in A/\sim$有

$$\begin{aligned}&h(\overline{o_i}([a_1],[a_2],\cdots,[a_{k_i}]))=h([o_i(a_1,a_2,\cdots,a_{k_i})])\\&=\varphi(o_i(a_1,a_2,\cdots,a_{k_i}))=o'_i(\varphi(a_1),\varphi(a_2),\cdots,\varphi(a_{k_i}))\\&=o'_i(h([a_1]),h([a_2]),\cdots,h([a_{k_i}])).\end{aligned}$$

所以有$V_1/\sim\ \overset{h}{\cong}\langle\varphi(A),o'_1,o'_2,\cdots,o'_r\rangle$. ∎

同态基本定理告诉我们,任何代数系统V的商代数是它的一个同态像.反过来,如果V'是V的同态像,则V'与V的一个商代数是同构的.从抽象代数的观点看,V'就是V的商代数.

【例1.29】　设$V=\langle Z_6,\oplus\rangle$,其中$Z_6=\{0,1,\cdots,5\}$,$\oplus$为模6加法.试用同余类描述$V$上所有的同余关系.

解　根据例1.25,V上有6个自同态,即$\varphi: Z_6\rightarrow Z_6$,$\varphi_p(x)=(px)\text{mod}6$,$p=0,1,\cdots,5$.考虑$V$的同态像.$\varphi_0(x)=0$,$\forall x\in Z_6$,$V$在$\varphi_0$下的同态像是$\langle\{0\},\oplus\rangle$.$\varphi_1(x)=x$,$\varphi_5(x)=(5x)\text{mod}6$,$\forall x\in Z_6$,$V$在$\varphi_1$和$\varphi_5$下的同态像是$V$自己.$\varphi_2(x)=(2x)\text{mod}6$,$\varphi_4(x)=(4x)\text{mod}6$,$\forall x\in Z_6$,$V$在$\varphi_2$和$\varphi_4$下的同态像是$\langle\{0,2,4\},\oplus\rangle$.$\varphi_3(x)=(3x)\text{mod}6$,$\forall x\in Z_6$,$V$在$\varphi_3$下的同态像是$\langle\{0,3\},\oplus\rangle$.根据同态基本定理,$V$有4个商代数,因此$V$上有4个不同的同余关系,分别由$\varphi_0,\varphi_1,\varphi_2,\varphi_3$导出.它们的同余类分别是:

由 φ_0 导出的同余关系，同余类是$\{0,1,\cdots,5\}$；

由 φ_1 导出的同余关系，同余类是$\{0\},\{1\},\cdots,\{5\}$；

由 φ_2 导出的同余关系，同余类是$\{0,3\},\{1,4\},\{2,5\}$；

由 φ_3 导出的同余关系，同余类是$\{0,2,4\},\{1,3,5\}$.

§1.5 Σ代数

到目前为止我们已经对代数系统有了基本的了解，但实际当中存在的许多代数系统更为复杂.它的载体可能不是一个集合而是一个集合族，运算也不是一个集合上的运算而是在不同的集合之间的运算.换句话说，运算数与运算结果属于集合族中不同的集合.这样的代数系统叫做Σ代数或分类代数.

定义 1.19 一个**Σ代数** V 是一个二元组$\langle F,\Omega\rangle$，其中 F 是一个非空集合构成的集合族，$\forall A\in F$，称 A 是 V 的**基集**. Ω 是一个非空的运算集，$\forall o\in\Omega$，$o: A_{i_1}\times A_{i_2}\times\cdots\times A_{i_n}\to A_i$，$A_{i_1},A_{i_2},\cdots,A_{i_n},A_i\in F$，$n\in N$.

使用Σ代数可以给出抽象数据类型(ADT)的代数规范.从传统的数据结构到抽象数据类型的使用是软件系统设计的新发展.把一类数据和数据上的操作封装在一起就构成了一个抽象数据类型.在给出抽象数据类型的规范时并不需要说明数据结构的具体表示和操作的实现方法.下面给出的是一个自然数栈的代数描述.

【例 1.30】

sorts Stack; Nature; Bool;

operations

  true, false: → Bool;

  zero: → Nature;

  succ: Nature → Nature;

  emptystack: → Stack;

  isempty: Stack → Bool;

push: Stack × Nature → Stack;

pop: Stack → Stack;

top: Stack → Nature;

declare s: Stack; n: Nature;

axioms

isempty(emptystack) = true;

isempty(push(s,n)) = false;

pop (emptystack) = emptystack;

pop (push(s,n)) = s;

top (emptystack) = zero;

top (push(s,n)) = n.

这是一个 Σ 代数,$V = \langle F,\Omega \rangle$, 其中 F = {Stack, Nartue, Bool}, Ω = {true, false, zero, succ, emptystack, isempty, push, pop, top}, declare 部分给出了在公理部分所使用的变量说明, axioms 部分规范了这个 Σ 代数的性质.

Σ 代数是一般代数系统的推广. 前边关于一般代数系统的许多概念,如子代数、积代数、代数系统的同态与同构、同余关系和商代数等都可以运用到 Σ 代数中去. 因篇幅所限这里就不再介绍了,有兴趣的读者可以参考有关的书籍.

习 题 一

1. 设 $\oplus$, $\otimes$ 分别为 Z_4 上的模 4 加法和乘法,给出 $\oplus$ 和 $\otimes$ 的运算表.

2. 设 $A = \{0,1\}$, $\circ$ 为函数的合成运算,试给出 A 上所有的函数关于$\circ$运算的运算表.

3. 设 $A = \{1,2,\cdots,n\}$, τ 为 A 上的一元运算. $\forall i \in A$ 有 $\tau(i) = (i+1)\mathrm{mod}n$. 称代数系统$\langle A,\tau \rangle$为时钟代数. 当 $n = 5$ 时给出 τ 的运算表.

4. 判断下列集合对所给的代数运算是否封闭. 如果封闭,则指明该集合上

的二元运算是否满足交换律、结合律、幂等律、消去律、分配律和吸收律，并找出该运算的单位元和零元.

(1) 整数集合 Z 和普通的减法运算；

(2) 非零整数集合 Z^* 和普通的乘法运算；

(3) 集合 $A = \{x \mid x \in N \land x$ 为奇数$\}$ 和普通的加法及乘法运算；

(4) n 阶实矩阵集合 $M_n(R)$ 关于矩阵加法和矩阵乘法运算；

(5) n 阶实可逆矩阵的集合关于矩阵加法和矩阵乘法运算；

(6) 集合 $nZ = \{nk \mid k \in Z\}, n \in Z^+$，关于普通加法和乘法运算；

(7) 正实数集R^+和$\circ$运算，其中$\circ$运算定义为$a \circ b = ab - a - b, \forall a,b \in R^+$；

(8) 集合 $A = \{a_1, a_2, \cdots, a_n\}$，$n \geqslant 1$，$\circ$ 运算为 $a \circ b = b$，$\forall a,b \in A$；

(9) 集合 A 上的所有二元关系的集合 $R(A)$ 和关系的合成运算；

(10) 正整数集 Z^+ 和求两个数的最大公约数及最小公倍数的运算.

5. 设 $A = \{a,b,c\}, a,b,c \in R$. 能否确定 a,b,c 的值使得

(1) A 对普通加法封闭；

(2) A 对普通乘法封闭.

6. $S = \{f \mid f$ 是$[a,b]$上的连续函数$, a,b \in R\}$ 问S关于下面的每个运算是否构成代数系统?如果能构成代数系统，说明该运算是否适合交换律和结合律，并求出单位元和零元.

(1) 函数加法，即$(f+g)(x) = f(x) + g(x)$，$\forall x \in [a,b]$；

(2) 函数减法，即$(f-g)(x) = f(x) - g(x)$，$\forall x \in [a,b]$；

(3) 函数乘法，即$(f \cdot g)(x) = f(x) \cdot g(x)$，$\forall x \in [a,b]$；

(4) 函数除法，即$(f/g)(x) = f(x)/g(x)$，$\forall x \in [a,b]$.

7. 判断正整数集 Z^+ 和下面每个二元运算$\circ$是否构成代数系统. 如果是，则说明这个运算是否适合交换律、结合律和幂等律，并求出单位元和零元.

(1) $a \circ b = \max\{a,b\}$；

(2) $a \circ b = \min\{a,b\}$；

(3) $a \circ b = a^b$；

(4) $a \circ b = (a/b) + (b/a)$.

8. 设 p,q,r 是实数，$\circ$ 为 R 上的二元运算. $\forall a,b \in R, a \circ b = pa + qb + r$. 问$\circ$运算是否适合交换律、结合律和幂等律，是否有单位元和零元，并证明你的结论.

9. 设 $*$ 为有理数集 Q 上的二元运算，$\forall x,y \in Q$ 有 $x*y = x+y-xy$. 说明 $*$ 运算是否适交换律、结合律和幂等律，并求出 Q 中关于 $*$ 运算的单位元、零元及所有可逆元素的逆元.

10. 设 $A=\{a,b\}$，试给出 A 上所有的二元运算和一元运算，并找出一个既不可交换也不可结合的二元运算.

11. 设 $A=Q\times Q$，Q 为有理数集，$\circ$ 为 A 上的二元运算. $\forall\langle a,b\rangle,\langle c,d\rangle\in A$ 有

$$\langle a,b\rangle\circ\langle c,d\rangle=\langle ac,ad+b\rangle,$$

说明$\circ$运算是否适合交换律和结合律. 并求出 A 中关于$\circ$运算的单位元、零元和所有可逆元素的逆元.

12. 设代数系统 $V=\langle A,\circ\rangle$，其中$\circ$运算由运算表(见表 1.6)给出. 说明$\circ$运算是否满足交换律、结合律和幂等律，并确定 A 中关于$\circ$运算的单位元和零元.

表 1.6

(1)

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(2)

$\circ$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

(3)

$\circ$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

(4)

$\circ$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	b

13. 证明定理 1.3.

14. $V=\langle Z_6,\oplus\rangle$，$\oplus$ 为模 6 加法. 指出 V 的所有的子代数，并说明哪些子代数是平凡的子代数，那些是真子代数.

15. 设 $V_1=\langle\{1,2,3\},\circ,1\rangle$，$\forall x,y\in\{1,2,3\}$，$x\circ y=\max\{x,y\}$，$V_2=\langle\{5,6\},*,6\rangle$，$\forall a,b\in\{5,6\}$，$a*b=\min\{a,b\}$.

(1) 给出积代数 $V_1\times V_2$ 的运算表和特异元素；

(2) 给出 V_1 的所有的子代数.

16. 代数系统 $V_1=\langle Z_3,\oplus_3\rangle$，$V_2=\langle Z_2,\oplus_2\rangle$，其中 $\oplus_3$ 和 $\oplus_2$ 分别为模 3 和

模 2 加法.

(1) 给出积代数 $V_1 \times V_2$ 的运算表;

(2) 求出积代数 $V_1 \times V_2$ 的单位元和每个可逆元素的逆元.

17. 证明定理 1.6.

18. 设 V_1 是复数集 C 关于复数加法和复数乘法构成的代数系统, $V_2 = \langle B, +, \cdot \rangle$, 其中

$$B = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in R \right\},$$

$+$ 和 $\cdot$ 分别为矩阵加法和乘法. 证明 V_1 同构于 V_2.

19. 设 $V_1 = \langle A, o_1, o_2 \rangle$, $V_2 = \langle B, \overline{o_1}, \overline{o_2} \rangle$ 是含有两个二元运算的代数系统. 证明积代数 $V_1 \times V_2$ 和 $V_2 \times V_1$ 同构.

20. 设 $V_1 = \langle P(\{a,b\}), \cup, \cap, \sim, \varnothing, \{a,b\} \rangle$, $V_2 = \langle \{0,1\}, +, \cdot, -, 0, 1 \rangle$, 其中 $+, \cdot, -$ 分别为布尔加、乘和补运算. 令 $\varphi: P(\{a,b\}) \to \{0,1\}$, 且 $\forall x \in P(\{a,b\})$, 别定义如下

$$\varphi(x) = \begin{cases} 1, & a \in x; \\ 0, & a \notin x. \end{cases}$$

证明 φ 为 V_1 到 V_2 的满同态.

21. 证明定理 1.8.

22. 设 $V_1 = \langle A, \circ \rangle$, $V_2 = \langle B, * \rangle$, $V_3 = \langle C, \cdot \rangle$ 是含有一个二元运算的代数系统. $\varphi_1: A \to B$ 是 V_1 到 V_2 的同态, $\varphi_2: B \to C$ 是 V_2 到 V_3 的同态. 证明 $\varphi_2 \circ \varphi_1$ 是 V_1 到 V_3 的同态.

23. 证明对任意的代数系统 V_1, V_2, V_3 有

(1) $V_1 \cong V_1$;

(2) 若 $V_1 \cong V_2$, 则 $V_2 \cong V_1$;

(3) 若 $V_1 \cong V_2$, $V_2 \cong V_3$, 则 $V_1 \cong V_3$.

24. 设 $V_1 = \langle C, \cdot \rangle$, $V_2 = \langle R, \cdot \rangle$ 是代数系统, $\cdot$ 为普通乘法. 下面哪个函数 φ 是 V_1 到 V_2 的同态? 如果 φ 是同态, 求出 V_1 在 φ 下的同态像.

(1) $\varphi: C \to R$, $\varphi(z) = |z| + 1$, $\forall z \in C$;

(2) $\varphi: C \to R$, $\varphi(z) = |z|$, $\forall z \in C$;

(3) $\varphi: C \to R$, $\varphi(z) = 0$, $\forall z \in C$;

(4) $\varphi: C \to R$, $\varphi(z) = 2$, $\forall z \in C$.

25. 设$V=\langle A,\cdot\rangle$,其中$A=\{5^n|n\in Z^+\}$,·为普通乘法.试求出所有V上的自同构.

26. 设代数系统$V_1=\langle Z^+,\cdot\rangle$,$V_2=\langle Z_2,\cdot\rangle$,其中·为普通乘法.定义$\varphi$: $Z^+\to Z_2$,$\forall x\in Z^+$有

$$\varphi(x)=\begin{cases}1, & x=1;\\ 0, & x>1.\end{cases}$$

证明φ是V_1到V_2的满同态.

27. 设$V=\langle Z,+\rangle$,判断下面给出的二元关系R是否为V上的同余关系,并说明理由.

(1) $\forall x,y\in Z$, $xRy\Leftrightarrow x$与y同号或$x=y=0$;

(2) $\forall x,y\in Z$, $xRy\Leftrightarrow |x-y|<5$;

(3) $\forall x,y\in Z$, $xRy\Leftrightarrow x=y=0$或$x\neq 0$, $y\neq 0$;

(4) $\forall x,y\in Z$, $xRy\Leftrightarrow x\geqslant y$.

28. 证明定理1.9.

29. 设$V_1=\langle Z,\triangle\rangle$,$V_2=\langle Z_2,\overline{\triangle}\rangle$是含有一元运算的代数系统,其中$\triangle$和$\overline{\triangle}$分别定义如下:

$$\triangle x=x+1,\ \forall x\in Z,\quad \overline{\triangle}y=(y+1)\bmod 2,\ \forall y\in Z_2.$$

令

$$\varphi: Z\to Z_2,\ \varphi(a)=(a)\bmod 2,\ \forall a\in Z.$$

(1) 证明φ是V_1到V_2的同态;

(2) 给出φ在V_1上导出的划分.

30. 设$V_1=\langle A_k,+\rangle$, $V_2=\langle A_m,+\rangle$,其中

$$A_j=\{x|x\in Z且x\geqslant j\},\quad j,k,m,n\in N,\quad nk\geqslant m,$$

+为普通加法.令φ: $A_k\to A_m$, $\varphi(x)=nx$, $\forall x\in A_k$.

(1) 证明φ是V_1到V_2的同态;

(2) 令~表示由φ导出的V_1上的同余关系,试描述商代数$V_1/\sim$(给出集合和运算表).

31. 设代数系统$V=\langle A,\circ\rangle$,其中$A=\{a,b,c,d\}$,$\circ$由运算表(表1.7)给出.

(1) 试给出V的所有的自同态;

(2) 试给出V上所有的同余关系.

表 1.7

$\circ$	a	b	c	d
a	b	a	b	b
b	b	b	b	b
c	b	b	b	b
d	b	b	b	b

32. 设 $V_1=\langle A,*,\vartriangle,k\rangle$，$V_2=\langle B,\circ,\bar{\vartriangle},\bar{k}\rangle$ 是代数系统，其中 $*$ 和 $\circ$ 为二元运算，$\vartriangle$ 和 $\bar{\vartriangle}$ 为一元运算，k 和 $\bar{k}$ 为零元运算. 在积代数 $V_1\times V_2$ 上定义二元关系 R，$\forall\langle a,b\rangle,\langle c,d\rangle\in A\times B$ 有

$$\langle a,b\rangle R\langle c,d\rangle\Leftrightarrow a=c.$$

(1) 证明 R 为 $V_1\times V_2$ 上的同余关系；

(2) 证明 $V_1\times V_2/R\cong V_1$.

第二章　半群与独异点

§2.1　半群与独异点

半群和独异点是具有一个二元运算的代数系统.

定义 2.1　(1) 设$\circ$是集合 S 上的二元运算,若$\circ$运算在 S 上是可结合的,则称代数系统 $V = \langle S,\circ\rangle$ 是**半群**.

(2) 设 $V = \langle S,\circ\rangle$ 是半群,若存在 $e \in S$ 为 V 中关于$\circ$运算的单位元,则称 $V = \langle S,\circ,e\rangle$ 是**独异点**.

【例 2.1】

(1) 自然数集 N,整数集 Z,有理数集 Q,实数集 R 关于普通加法或乘法都可以构成半群和独异点. 正整数集 Z^+ 关于普通乘法可以构成半群和独异点,而关于加法只能构成半群.

(2) 设 $n \geqslant 2$,n 阶实矩阵集合 $M_n(R)$ 关于矩阵加法或矩阵乘法都能构成半群和独异点.

(3) 幂集 $P(B)$ 关于集合的并、交和对称差运算都可以构成半群和独异点.

(4) A^A 关于函数的合成运算构成了半群和独异点.

(5) $A = \{a_1,a_2,\cdots,a_n\}$,$n \in Z^+$,$\circ$为 A 上的二元运算. $\forall a_i,a_j \in A$ 有 $a_i\circ a_j = a_i$,则 A 关于$\circ$运算构成半群.

定义 2.2　设 $V = \langle S,\circ\rangle$ 是半群,$\forall x \in S$,$n \in Z^+$,定义 x 的 n 次幂 x^n 为:

$$x^1 = x,$$
$$x^{n+1} = x^n\circ x, \qquad n \in Z^+.$$

例如在半群$\langle Z, +\rangle$中,$\forall x \in Z$,x 的 n 次幂是$\underbrace{x + x + \cdots + x}_{n个x} = nx$. 而在半群$\langle P(B), \oplus\rangle$中,$\forall x \in P(B)$,$x$ 的 n 次幂是

$$\underbrace{x \oplus x \oplus \cdots \oplus x}_{n\text{个}x} = \begin{cases} \varnothing, & n \text{ 为偶数;} \\ x, & n \text{ 为奇数.} \end{cases}$$

半群中元素的幂运算遵从下面的规律.

定理 2.1 设 $V = \langle S, \circ \rangle$ 是半群，则 $\forall x, y \in S$ 有

(1) $x^n \circ x^m = x^{n+m}$;

(2) $(x^n)^m = x^{nm}$,

其中 $n, m \in Z^+$.

证 (1) 固定 n，施归纳于 m.

若 $m = 1$，则 $x^n \circ x^1 = x^n \circ x = x^{n+1}$.

假设对 $m = k$ 有 $x^n \circ x^k = x^{n+k}$ 成立，则对 $m = k+1$ 有

$$x^n \circ x^{k+1} = x^n \circ (x^k \circ x) = (x^n \circ x^k) \circ x = x^{n+k} \circ x = x^{n+k+1} = x^{n+(k+1)},$$

根据数学归纳法，对一切 $n, m \in Z^+$，结论为真.

(2) 固定 n，施归纳于 m.

$m = 1$ 时有 $(x^n)^1 = x^n = x^{n \cdot 1}$.

假设当 $m = k$ 时有 $(x^n)^k = x^{nk}$，则 $m = k+1$ 时有

$$(x^n)^{k+1} = (x^n)^k \circ x^n = x^{nk} \circ x^n = x^{nk+n} = x^{n(k+1)},$$

根据数学归纳法，对一切 $n, m \in Z^+$，结论为真. ∎

可以将 x 的 n 次幂的概念从半群推广到独异点. 在独异点 $V = \langle S, \circ, e \rangle$ 中，$\forall x \in S, n \in N$，x 的 n 次幂是：

$$x^0 = e,$$
$$x^{n+1} = x^n \circ x, \quad \text{其中 } n \in N.$$

不难证明定理 2.1 的结论在独异点中也成立，只是 m, n 不仅限于正整数，也可以是 0.

定理 2.2 设 $\langle S, \circ \rangle$ 是半群，则可以适当地定义单位元 e，将这个半群扩张为独异点 $\langle S', \circ', e \rangle$.

证 任取 e 使得 $e \notin S$. 令 $S' = S \cup \{e\}$，且定义 S' 上的二元运算 $\circ'$ 如下：

$$\forall x, y \in S, \; x \circ' y = x \circ y,$$

$$\forall x \in S,\ x \circ' e = e \circ' x = x,$$
$$e \circ' e = e.$$

易见$\circ'$运算在S'上是可结合的，且单位元为e. 因此$\langle S', \circ', e\rangle$是独异点. ∎

下面考虑半群和独异点的子代数.

定义 2.3 半群S的子代数叫做S的**子半群**. 独异点T的子代数叫做T的**子独异点**.

【例 2.2】 设$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in R \right\}$，则$A$关于矩阵乘法构成半群$\langle A, \cdot\rangle$，且它是$\langle M_2(R), \cdot\rangle$的子半群. 令$V = \left\langle A, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\rangle$，则$V$是一个独异点，但它不是$\left\langle M_2(R), \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$的子独异点. 因为$M_2(R)$中关于·运算的单位元不属于$A$.

定理 2.3 设S为半群，V为独异点，则S的任何子半群的非空交集仍是S的子半群，V的任何子独异点的交集仍是V的子独异点.

证 设$\bigcap_i S_i$是S的子半群的非空交集，$\forall x, y \in \bigcap_i S_i$，则$x, y$属于每个$S_i$，因为$S_i$是$S$的子半群，所以$xy \in S_i$. 这就证明了$xy \in \bigcap_i S_i$. 根据子代数定义$\bigcap_i S_i$是$S$的子代数，即子半群.

令$\bigcap_i V_i$是独异点V的子独异点的交集. 设V的单位元为e，因为V_i是V的子代数，故$\forall i$有$e \in V_i$，所以$e \in \bigcap_i V_i$，$\bigcap_i V_i$非空. 再根据上面的证明可知$\bigcap_i V_i$是V的子独异点. ∎

由以上定理可知，若干个子半群的非空交集仍是子半群，但它们的并不一定是子半群. 例如$2Z = \{2k \mid k \in Z\}$，$3Z = \{3k \mid k \in Z\}$都是$\langle Z, +\rangle$的子半群，但$2Z \cup 3Z$并不是$\langle Z, +\rangle$的子半群.

定义 2.4 设S为半群，B是S的非空子集，则S的所有包含B的子半群的交仍是S的子半群，称为**由B生成的子半群**，记作$\langle B\rangle$.

定理 2.4 S为半群，B是S的非空子集. $\forall n \in Z^+$，令

$$B^n = \{b_1b_2\cdots b_n \mid b_i \in B, i = 1,2,\cdots,n\},$$

则

$$\langle B\rangle = \bigcup_{n\in Z^+} B^n.$$

证 先证 $\bigcup_{n\in Z^+} B^n \subseteq \langle B\rangle$. 任取 $x \in \bigcup_{n\in Z^+} B^n$,则存在 $n \in Z^+$ 且 $x \in B^n$,因此 $x = b_1b_2\cdots b_n$ 且 $b_i \in B, i = 1,2,\cdots,n$. 因为 $B \subseteq \langle B\rangle$,所以 $x = b_1b_2\cdots b_n$ 且 $b_i \in \langle B\rangle, i = 1,2,\cdots,n$;又由于$\langle B\rangle$是子半群,因此 $x = b_1b_2\cdots b_n \in \langle B\rangle$.

再证$\langle B\rangle \subseteq \bigcup_{n\in Z^+} B^n$. 任取 $x \in B$,则 $x \in B^1$,所以 $x \in \bigcup_{n\in Z^+} B^n$. 这就证明了 $B \subseteq \bigcup_{n\in Z^+} B^n$. 易证 $\bigcup_{n\in Z^+} B^n$ 是 S 的非空子集且关于 S 中的运算封闭,是 S 的子半群. 由于$\langle B\rangle$ 是 S 中所有包含 B 的子半群的交,所以$\langle B\rangle \subseteq \bigcup_{n\in Z^+} B^n$. ∎

半群与独异点的积代数称为**积半群和积独异点**. 有关积代数的定理和性质都可以用于积半群与积独异点.

类似地可以把一般代数系统的同态与商代数的概念用到半群和独异点上,从而得到**商半群与商独异点**. 有关同态,同余关系和商代数的一般定理对半群和独异点也是正确的.

定理 2.5 设 $V = \langle S, *\rangle$ 为半群,$V' = \langle S^S, \circ\rangle$,$\circ$为函数的合成运算,则 V' 是半群,且存在 V 到 V' 的同态.

证 V' 是半群,因为S^S关于合成运算$\circ$是封闭的,且合成运算适合结合律. 定义 $f_a: S \to S$,且 $f_a(x) = a * x$, $\forall x \in S$,则 $f_a \in S^S$. 令

$$\varphi: S \to S^S,\ \varphi(a) = f_a,\ \forall a \in S,$$

则 φ是 V 到 V' 的同态. 因为 $\forall a,b \in S$ 有

$$\varphi(a * b) = f_{a*b},\quad \varphi(a)\circ\varphi(b) = f_a\circ f_b.$$

我们只须证明 $\forall x \in S$ 有 $f_{a*b}(x) = f_a\circ f_b(x)$ 即可.

$$f_{a*b}(x) = (a * b) * x = a * (b * x) = f_a(f_b(x)) = f_a\circ f_b(x),$$

所以有 $\varphi(a * b) = \varphi(a) \circ \varphi(b)$. ∎

定理 2.6 设 $V = \langle S, *, e\rangle$ 是独异点，则存在 $T \subseteq S^S$ 使 $\langle T, \circ, I_S\rangle$ 同构于 $\langle S, *, e\rangle$.

证 类似于定理 2.5，令 φ: $S \to S^S$, $\varphi(a) = f_a$, $\forall a \in S$, 则 $\forall a, b \in S$ 有 $\varphi(a * b) = \varphi(a) \circ \varphi(b)$. 此外

$$\varphi(e) = f_e = I_S,$$

所以 φ 是 $\langle S, *, e\rangle$ 到 $\langle S^S, \circ, I_S\rangle$ 的同态.

任取 $a, b \in S$，若 $\varphi(a) = \varphi(b)$，即 $f_a = f_b$，则 $\forall x \in S$ 有

$$a * x = f_a(x) = f_b(x) = b * x.$$

令 $x = e$，就得到 $a = b$，所以 φ 是单射的.

令 $T = \varphi(S)$，则 $T \subseteq S^S$ 且 φ: $S \to T$ 是双射的，因此有 $\langle S, *, e\rangle$ 同构于 $\langle T, \circ, I_S\rangle$. ∎

这个定理说明任何独异点都是一个变换的独异点，因此定理 2.6 叫做独异点的表示定理.

§2.2 有穷自动机

有穷自动机在形式语言方面有着重要的应用. 我们先给出有穷半自动机和自动机的定义.

定义 2.5 (1) 一个**有穷半自动机**是一个三元组 $M = \langle Q, \Sigma, \delta\rangle$，其中 Q 为有穷状态集，Σ 为有穷输入字符表，δ: $Q \times \Sigma \to Q$ 为状态转移函数.

(2) 一个**有穷自动机**是一个五元组 $M = \langle Q, \Sigma, \Gamma, \delta, \lambda\rangle$，其中 Q，Σ 和 δ 的定义如(1)，Γ 为有穷输出字符表，λ: $Q \times \Sigma \to \Gamma$ 为输出函数.

为了书写的简便，今后将 $\delta(\langle q, a\rangle)$ 记为 $\delta(q, a)$，$\lambda(\langle q, a\rangle)$ 记为 $\lambda(q, a)$.

设 M 是有穷半自动机，$q_0 \in Q$ 是初始状态. $w = a_0a_1\cdots a_{n-1}$ 是长为 n 的输入串. 若 $\delta(q_j, a_j) = q_{j+1}$, $j = 0, 1, \cdots, n-1$，则 M 从 q_0 出

始，经过 n 步最终达到 q_n. 这样就得到一个工作在 Σ^* 上的半自动机 M^*，称为 M **的扩展**.

定义 2.6　设 $M = \langle Q,\Sigma,\delta \rangle$ 是有穷半自动机，则 M 可以扩展成 $M^* = \langle Q,\Sigma^*,\delta^* \rangle$，其中 Σ^* 是 Σ 上的串的集合，$\delta^*: Q \times \Sigma^* \to Q$，$\forall a_0a_1\cdots a_n \in \Sigma^*$ 有

$$\delta^*(q, \Lambda) = q,$$

$$\delta^*(q,a_0) = \delta(q,a_0),$$

$$\delta^*(q,a_0a_1\cdots a_n) = \delta(\delta^*(q,a_0a_1\cdots a_{n-1}),a_n), \quad 1 \leqslant n.$$

和以上定义类似，也可以定义扩展的有穷自动机 $M^* = \langle Q,\Sigma^*,\Gamma^*,\delta^*,\lambda^* \rangle$，其中 Q,Σ^*,δ^* 与有穷半自动机一样，Γ^* 是 Γ 上的串的集合，λ^* 定义如下. $\lambda^*: Q \times \Sigma^* \to \Gamma^*$，$\forall a_0a_1\cdots a_n \in \Sigma^*$ 有

$$\lambda^*(q, \Lambda) = \Lambda,$$

$$\lambda^*(q,a_0) = \lambda(q,a_0),$$

$$\lambda^*(q,a_0a_1\cdots a_n) = \lambda(q,a_0)\lambda^*(\delta(q,a_0),a_1\cdots a_n), \ 1 \leqslant n.$$

可以证明扩展的有穷自动机具有下面的性质.

定理 2.7　设 $M^* = \langle Q,\Sigma^*,\Gamma^*,\delta^*,\lambda^* \rangle$ 是扩展的有穷自动机，则 $\forall w_1,w_2 \in \Sigma^*$ 有

(1) $\delta^*(q,w_1w_2) = \delta^*(\delta^*(q,w_1),w_2)$,

(2) $\lambda^*(q,w_1w_2) = \lambda^*(q,w_1)\lambda^*(\delta^*(q,w_1),w_2)$,

其中 w_1w_2 是 w_1 与 w_2 的连接.

证　(1) 令 $w_1 = a_0a_1\cdots a_{m-1}, w_2 = b_0b_1\cdots b_{n-1}$，任意给定 w_1 的长度 $m \in N$，对 w_2 的长度 n 进行归纳.

$n = 0$，则 $w_2 = \Lambda$，因此有

$$\begin{aligned}\delta^*(q,w_1w_2) &= \delta^*(q,w_1) = \delta^*(\delta^*(q,w_1), \Lambda) \\ &= \delta^*(\delta^*(q,w_1),w_2).\end{aligned}$$

假设 $n = k$ 时结论成立，即有

$$\delta^*(q,a_0a_1\cdots a_{m-1}b_0b_1\cdots b_{k-1}) = \delta^*(\delta^*(q,a_0a_1\cdots a_{m-1}),b_0b_1\cdots b_{k-1}).$$

则当 $n=k+1$ 时 $w_2=b_0b_1\cdots b_k$，因此有

$$\begin{aligned}&\delta^*(q,w_1w_2)\\=&\delta^*(q,a_0a_1\cdots a_{m-1}b_0b_1\cdots b_k)\\=&\delta(\delta^*(q,a_0a_1\cdots a_{m-1}b_0b_1\cdots b_{k-1}),\ b_k)\\=&\delta(\delta^*(\delta^*(q,a_0a_1\cdots a_{m-1}),b_0b_1\cdots b_{k-1}),\ b_k)\\=&\delta^*(\delta^*(q,a_0a_1\cdots a_{m-1}),b_0b_1\cdots b_{k-1}\ b_k)\\=&\delta^*(\delta^*(q,w_1),w_2).\end{aligned}$$

(2) 任意给定 w_2 的长度 $n\in N$，对 w_1 的长度 m 进行归纳.

$m=0$，则 $w_1=\Lambda$，因此有

$$\begin{aligned}&\lambda^*(q,w_1w_2)=\lambda^*(q,w_2)=\Lambda\ \lambda^*(q,w_2)\\=&\lambda^*(q,\ \Lambda)\lambda^*(\delta^*(q,\ \Lambda),w_2)\\=&\lambda^*(q,w_1)\lambda^*(\delta^*(q,w_1),w_2).\end{aligned}$$

假设 $m=k$ 时结论成立，即当 $w_1=a_1a_2\cdots a_k$ 有

$$\begin{aligned}&\lambda^*(q,a_1a_2\cdots a_kb_0b_1\cdots b_{n-1})\\=&\lambda^*(q,a_1a_2\cdots a_k)\lambda^*(\delta^*(q,a_1a_2\cdots a_k),b_0b_1\cdots b_{n-1}).\end{aligned}$$

则当 $w_1=a_0a_1\cdots a_k$ 时有

$$\begin{aligned}&\lambda^*(q,w_1w_2)=\lambda^*(q,a_0a_1\cdots a_kb_0b_1\cdots b_{n-1})\\=&\lambda(q,a_0)\ \lambda^*(\delta(q,a_0),a_1\cdots a_kb_0b_1\cdots b_{n-1})\\=&\lambda(q,a_0)\ \lambda^*(\delta(q,a_0),a_1\cdots a_k)\\&\lambda^*(\delta^*(\delta(q,a_0),a_1\cdots a_k),b_0b_1\cdots b_{n-1})\\=&\lambda(q,a_0)\ \lambda^*(\delta(q,a_0),a_1\cdots a_k)\\&\lambda^*(\delta^*(\delta^*(q,a_0),a_1\cdots a_k),b_0b_1\cdots b_{n-1})\\=&\lambda^*(q,a_0a_1\cdots a_k)\ \lambda^*(\delta^*(q,a_0a_1\cdots a_k),\ b_0b_1\cdots b_{n-1})\\=&\lambda^*(q,w_1)\ \lambda^*(\delta^*(q,w_1),w_2).\end{aligned}$$ ∎

以上定理的结论(1)对半自动机的扩展 $M^*=\langle Q,\Sigma^*,\delta^*\rangle$ 也成立.

下面研究半自动机 M 和独异点的关系. 不难证明任意给定半自

动机 M，可以得到一个对应的独异点 T_M；反之，任意给定独异点 T，可以得到一个对应的半自动机 M_T。请看下面的定理.

定理 2.8　设 $M = \langle Q,\Sigma,\delta\rangle$ 是半自动机，$M^* = \langle Q,\Sigma^*,\delta^*\rangle$ 是 M 的扩展. 对任意的 $w \in \Sigma^*$，定义 $f_w: Q \to Q$，$f_w(q) = \delta^*(q,w)$. 令 $S = \{f_w | w \in \Sigma^*\}$ 是所有这样定义的函数的集合，$\circ$ 是函数的合成运算，则 $T_M = \langle S,\circ,f_\Lambda\rangle$ 是一个独异点，且是 $\langle Q^Q,\circ,I_Q\rangle$ 的子独异点.

证　先证 S 关于合成运算 $\circ$ 是封闭的. 任取 $f_{w_1},f_{w_2} \in S$，我们只须证明 $f_{w_1}\circ f_{w_2} \in S$ 即可. $\forall q \in Q$，

$$f_{w_1}\circ f_{w_2}(q) = f_{w_1}(f_{w_2}(q)) = f_{w_1}(\delta^*(q,w_2))$$

$$=\delta^*(\delta^*(q,w_2),w_1) = \delta^*(q,w_2w_1) = f_{w_2w_1}(q).$$

所以

$$f_{w_1}\circ f_{w_2} = f_{w_2w_1} \in S.$$

又由于合成运算 $\circ$ 是可结合的，所以 $\langle S,\circ\rangle$ 构成半群，且是 $\langle Q^Q,\circ\rangle$ 的子半群.

I_Q 是 $\langle Q^Q,\circ,I_Q\rangle$ 的单位元，为证明 $\langle S,\circ,f_\Lambda\rangle$ 是 $\langle Q^Q,\circ,I_Q\rangle$ 的子独异点，只须证明 $f_\Lambda = I_Q$ 即可. $\forall q \in Q$ 有 $f_\Lambda(q) = \delta^*(q,\Lambda) = q$，所以 $f_\Lambda = I_Q$.

∎

定理 2.9　设 $T = \langle S,\cdot,e\rangle$ 是独异点，则存在半自动机 M，且 M 所对应的独异点 T_M 同构于 T.

证　如下构造半自动机 $M = \langle Q,\Sigma,\delta\rangle$，其中 $Q = \Sigma = S$，$\delta: S \times S \to S$，$\delta(a,b) = b \cdot a$，$\forall a,b \in S$. 易见 $\Sigma^* = \Sigma = S$.

和定理 2.8 的证明类似，$\forall a \in \Sigma$ 定义 $f_a: S \to S$，$f_a(q) = \delta^*(q,a)$，$\forall q \in S$. 令 $A = \{f_a | a \in S\}$，则 $T_M = \langle A,\circ,f_e\rangle$ 是 M 所对应的独异点.

令 $\varphi: S \to A$，$\varphi(a) = f_a$，$\forall a \in S$. 先证明 φ 是 T 到 T_M 的同态. 任取 $a,b \in S$，$\forall q \in S$ 有

$$\varphi(a \cdot b)(q) = f_{a\cdot b}(q) = \delta^*(q,a \cdot b) = \delta(q,a \cdot b) = a \cdot b \cdot q,$$

$$\varphi(a)\circ\varphi(b)(q) = f_a(f_b(q)) = \delta^*(\delta^*(q,b),a)$$

$$= \delta(\delta(q,b),a) = a \cdot b \cdot q,$$

且有

$$\varphi(e) = f_e.$$

所以 φ 是 T 到 T_M 的同态.

其次证明 φ 是 S 到 A 的双射函数. 任取 $f_c \in A$, 有 $c \in S$, 使得 $\varphi(c) = f_c$, φ 是满射的. 假设有 $a,b \in S$, 且 $\varphi(a) = \varphi(b)$. 则 $\forall q \in S$ 有

$$f_a(q) = f_b(q) \Rightarrow \delta^*(q,a) = \delta^*(q,b)$$
$$\Rightarrow \delta(q,a) = \delta(q,b) \Rightarrow a \cdot q = b \cdot q.$$

令 $q = e$, 则有 $a = b$. 这就证明了 φ 是单射的. 因此有 $T \overset{\varphi}{\cong} T_M$. ∎

定理 2.8 和 2.9 证明了在半自动机和独异点之间存在着一一对应. 同样的情况对自动机也成立. 任给自动机 $M = \langle Q,\Sigma,\Gamma,\delta,\lambda\rangle$, 可以得到一个对应的独异点, 就是半自动机 $\langle Q,\Sigma,\delta\rangle$ 所对应的独异点. 反之, 任给一个独异点 $T = \langle S,\cdot,e\rangle$, 也可以得到一个对应的自动机 $M = \langle Q,\Sigma,\Gamma,\delta,\lambda\rangle$. 其中 Q,Σ,δ 与定理 2.9 中的定义一样, 而 $\Gamma = S$, λ: $S \times S \to S$, $\lambda(a,b) = b$, $\forall a,b \in S$. 那么有 $T_M \cong T$, 其中 T_M 就是 $\langle Q,\Sigma,\delta\rangle$ 所对应的独异点.

【例 2.3】 $T = \langle S,\cdot,1\rangle$ 是独异点, 其中 $S = \{1,-1\}$, $\cdot$ 为普通乘法. 和 T 对应的半自动机 $M = \langle\{1,-1\},\{1,-1\},\delta\rangle$, 其中状态转移函数 δ 如表 2.1 所示, M 的图给在图 2.1.

表 2.1

δ	1	−1
1	1	−1
−1	−1	1



图 2.1

根据定理 2.8, M 对应的独异点 $T_M = \langle\{f_1,f_{-1}\},\circ,f_1\rangle$. 其中 f_1 和 f_{-1} 定义如下:

f_1: $\{1,-1\} \to \{1,-1\}$, $f_1(1)=1$, $f_1(-1)=-1$.

f_{-1}: $\{1,-1\} \to \{1,-1\}$, $f_{-1}(1)=-1$, $f_{-1}(-1)=1$.

定义 φ: $\{1,-1\} \to \{f_1,f_{-1}\}$, $\varphi(1)=f_1$, $\varphi(-1)=f_{-1}$,则 φ 是 $T=\langle\{1,-1\},\cdot,1\rangle$ 到 $T_M=\langle\{f_1,f_{-1}\},\circ,f_1\rangle$ 的同构.

利用自动机和独异点的一一对应关系可以得到一系列有关自动机的性质.

定义 2.7 设 $M_1=\langle Q_1,\Sigma,\Gamma,\delta_1,\lambda_1\rangle$, $M_2=\langle Q_2,\Sigma,\Gamma,\delta_2,\lambda_2\rangle$ 是自动机,若有

(1) $Q_1 \subseteq Q_2$,

(2) $\delta_1=\delta_2 \upharpoonright (Q_1\times\Sigma)$,

(3) $\lambda_1=\lambda_2 \upharpoonright (Q_1\times\Sigma)$,

则称 M_1 是 M_2 的**子自动机**,记作 $M_1 \leqslant M_2$.

定理 2.10 设 $M_1=\langle Q_1,\Sigma_1,\Gamma_1,\delta_1,\lambda_1\rangle$, $M_2=\langle Q_2,\Sigma_2,\Gamma_2,\delta_2,\lambda_2\rangle$ 是自动机. 它们分别对应独异点 T_{M_1} 和 T_{M_2}. 若 $M_1\leqslant M_2$,则 T_{M_1} 是 T_{M_2} 的同态像.

证 设 $T_{M_1}=\langle A,\circ,f_\Lambda\rangle$,其中 $A=\{f_w \mid w\in\Sigma_1^*\}$,且 $\forall q_1\in Q_1$ 有 $f_w(q_1)=\delta_1^*(q_1,w)$, $T_{M_2}=\langle B,\circ,g_\Lambda\rangle$,其中 $B=\{g_\sigma \mid \sigma\in\Sigma_2^*\}$,且 $\forall q_2\in Q_2$ 有 $g_\sigma(q_2)=\delta_2^*(q_2,\sigma)$. 由于 $M_1\leqslant M_2$,易见 $\Sigma_1=\Sigma_2$, $\Gamma_1=\Gamma_2$,从而 $\Sigma_1^*=\Sigma_2^*$, $\Gamma_1^*=\Gamma_2^*$. 令

$$\varphi\colon B\to A,\ \varphi(g_\sigma)=f_\sigma,\ \forall g_\sigma\in B.$$

φ 是良定义的,因为

$g_w=g_\sigma \Rightarrow \forall q\in Q_2$ 有 $\delta_2^*(q,w)=\delta_2^*(q,\sigma)$

$\Rightarrow \forall q\in Q_1$ 有 $\delta_1^*(q,w)=\delta_1^*(q,\sigma)$ (由 $\delta_1=\delta_2\upharpoonright(Q_1\times\Sigma_1)$)

$\Rightarrow f_w=f_\sigma$.

φ 是满射的. 因为 $\forall f_w\in A$, $w\in\Sigma_1^*=\Sigma_2^*$,存在 $g_w\in B$,使得 $\varphi(g_w)=f_w$.

φ 是 T_{M_2} 到 T_{M_1} 的同态,因为 $\forall g_w, g_\sigma\in B$ 有

$$\varphi(g_w \circ g_\sigma) = \varphi(g_{\sigma w}) = f_{\sigma w} = f_w \circ f_\sigma = \varphi(g_w) \circ \varphi(g_\sigma),$$
$$\varphi(g_\Lambda) = f_\Lambda.$$
∎

下面考虑商自动机.

定义 2.8 $M = \langle Q, \Sigma, \Gamma, \delta, \lambda \rangle$ 是有穷自动机, $q_1, q_2 \in Q$, 若 $\forall w \in \Sigma^*$ 都有 $\lambda^*(q_1, w) = \lambda^*(q_2, w)$, 则称 q_1 和 q_2 是等价的, 记作 $q_1 \sim q_2$.

不难验证关系 $\sim$ 在 Q 上是自反的、对称的和传递的, 是 Q 上的等价关系.

定义 2.9 $M = \langle Q, \Sigma, \Gamma, \delta, \lambda \rangle$ 是有穷自动机, $\sim$ 为 Q 上的等价关系, 令 $\overline{M} = \langle Q/\sim, \Sigma, \Gamma, \overline{\delta}, \overline{\lambda} \rangle$, 使得

$\overline{\delta}$: $Q/\sim \times \Sigma \to Q/\sim$, $\overline{\delta}([q], a) = [\delta(q, a)]$,

$\overline{\lambda}$: $Q/\sim \times \Sigma \to \Gamma$, $\overline{\lambda}([q], a) = \lambda(q, a)$,

$$\forall [q] \in Q/\sim, \forall a \in \Sigma.$$

称 $\overline{M}$ 是 M 的**商自动机**.

为了验证商自动机 $\overline{M}$ 是良定义的, 我们需要证明下面两个条件: 对任意的 $[q_1], [q_2] \in Q/\sim$,

(1) $[q_1] = [q_2] \Rightarrow \overline{\delta}([q_1], a) = \overline{\delta}([q_2], a)$, $\forall a \in \Sigma$;

(2) $[q_1] = [q_2] \Rightarrow \overline{\lambda}([q_1], a) = \overline{\lambda}([q_2], a)$, $\forall a \in \Sigma$.

这就是说, $\overline{\delta}$ 和 $\overline{\lambda}$ 是关于类的运算, 必须与类的代表元素的选择无关.

证 先证(2). 任取 $[q_1], [q_2] \in Q/\sim$, $\forall a \in \Sigma$,

$[q_1] = [q_2] \Rightarrow q_1 \sim q_2 \Rightarrow \lambda^*(q_1, w) = \lambda^*(q_2, w), \forall w \in \Sigma^*$

$\Rightarrow \lambda^*(q_1, a) = \lambda^*(q_2, a) \Rightarrow \lambda(q_1, a) = \lambda(q_2, a)$

$\Rightarrow \overline{\lambda}([q_1], a) = \overline{\lambda}([q_2], a)$.

再证(1). 任取 $[q_1], [q_2] \in Q/\sim$, $\forall a \in \Sigma$,

$[q_1] = [q_2] \Rightarrow q_1 \sim q_2$

$\Rightarrow \lambda^*(q_1, aw) = \lambda^*(q_2, aw)$, $\forall w \in \Sigma^*$

$\Rightarrow \lambda(q_1, a)\lambda^*(\delta(q_1, a), w) = \lambda(q_2, a)\lambda^*(\delta(q_2, a), w), \forall w \in \Sigma^*$.

由(1)的证明可知 $q_1 \sim q_2 \Rightarrow \lambda(q_1,a)=\lambda(q_2,a)$. 根据两个序列相等的性质可推出

$$\lambda^*(\delta(q_1,a),w)=\lambda^*(\delta(q_2,a),w),\quad \forall w\in\Sigma^*.$$

因此有 $\delta(q_1,a)\sim\delta(q_2,a)$，而

$$\delta(q_1,a)\sim\delta(q_2,a)\Rightarrow[\delta(q_1,a)]=[\delta(q_2,a)]$$

$$\Rightarrow \bar{\delta}([q_1],a)=\bar{\delta}([q_2],a).$$ ∎

设 M_1,M_2 是有穷自动机，它们对应的独异点分别为 T_{M_1} 和 T_{M_2}. 可以证明，如果 M_2 是 M_1 的商自动机，则 T_{M_2} 同构于 T_{M_1} 的商独异点.

【例 2.4】 设 $M=\langle Q,\Sigma,\Gamma,\delta,\lambda\rangle$ 是有穷自动机，其中 $Q=\{q_0,q_1,\cdots,q_6\}$, $\Sigma=\{0,1\}$, $\Gamma=\{0,1\}$, δ 和 λ 的定义如表 2.2 所示. 可以验证在 Q 上的等价关系 $\sim$ 是：

$$q_1\sim q_3\sim q_6,$$

$$q_0\sim q_2,\ q_4\sim q_5.$$

M 的商自动机 $\overline{M}=\langle Q/\sim,\Sigma,\Gamma,\bar{\delta},\bar{\lambda}\rangle$, 其中 $Q/\sim=\{\{q_1,q_3,q_6\},\{q_0,q_2\},\{q_4,q_5\}\}=\{[q_1],[q_0],[q_4]\}$. $\bar{\delta}$ 和 $\bar{\lambda}$ 的定义如表 2.3 所示.

表 2.2

δ	0	1
q_0	q_1	q_2
q_1	q_0	q_3
q_2	q_6	q_0
q_3	q_0	q_1
q_4	q_5	q_1
q_5	q_4	q_3
q_6	q_2	q_6

λ	0	1
q_0	0	0
q_1	1	1
q_2	0	0
q_3	1	1
q_4	1	0
q_5	1	0
q_6	1	1

表 2.3

$\bar{\delta}$	0	1
$[q_1]$	$[q_0]$	$[q_1]$
$[q_0]$	$[q_1]$	$[q_0]$
$[q_4]$	$[q_4]$	$[q_1]$

$\bar{\lambda}$	0	1
$[q_1]$	1	1
$[q_0]$	0	0
$[q_4]$	1	0

不难看出，商自动机 $\overline{M}$ 保持了 M 的性质. 若以 q_0, $[q_0]$ 分别作为 M 和 $\overline{M}$ 的初始状态，则对任意的 $w\in\Sigma^*$, M 和 $\overline{M}$ 都会得到同样的输出. 这样的自动机称为等价的自动机.

定义 2.10 设 $M_1=\langle Q_1,\Sigma_1,\Gamma_1,\delta_1,\lambda_1\rangle$ 和 $M_2=\langle Q_2,\Sigma_2,\Gamma_2,\delta_2,$

$\lambda_2\rangle$ 是有穷自动机. 如果满足下述条件:

(1) $\Sigma_1 = \Sigma_2 = \Sigma$, $\Gamma_1 = \Gamma_2 = \Gamma$,

(2) $q_0 \in Q_1$, $q'_0 \in Q_2$ 分别为 M_1 和 M_2 的初始状态, 且 $\forall w \in \Sigma^*$ 都有 $\lambda_1^*(q_0, w) = \lambda_2^*(q'_0, w)$,

则称 M_1 和 M_2 是**等价的有穷自动机**, 记作 $M_1 \sim M_2$.

定理 2.11 设 $M_1 = \langle Q_1, \Sigma, \Gamma, \delta_1, \lambda_1\rangle$ 是有穷自动机, $M_2 = \langle Q_1/\sim, \Sigma, \Gamma, \delta_2, \lambda_2\rangle$ 是 M_1 的商自动机, 则 $M_1 \sim M_2$.

证 显然 M_1 和 M_2 的输入、输出字符集相等. 设 q_0 是 M_1 的初始状态, $q_0 \in Q_1$, 令 $[q_0] \in Q_1/\sim$ 是 M_2 的初始状态, 我们只须证明 $\forall w \in \Sigma^*$ 有

$$\lambda_1^*(q_0, w) = \lambda_2^*([q_0], w).$$

对 w 的长度进行归纳. 令 $w = a_0 a_1 \cdots a_n$.

当 $|w| = 1$ 时, $w = a_0$, 有

$$\lambda_1^*(q_0, a_0) = \lambda_1(q_0, a_0) = \lambda_2([q_0], a_0) = \lambda_2^*([q_0], a_0).$$

假设 $|w| = k$ 时等式成立, 即有

$$\lambda_1^*(q_0, a_1 a_2 \cdots a_k) = \lambda_2^*([q_0], a_1 a_2 \cdots a_k),$$

则当 $|w| = k + 1$ 时有

$$\lambda_1^*(q_0, a_0 a_1 \cdots a_k) = \lambda_1(q_0, a_0)\lambda_1^*(\delta_1(q_0, a_0), a_1 \cdots a_k),$$

$$\begin{aligned}
&\lambda_2^*([q_0], a_0 a_1 \cdots a_k) \\
&= \lambda_2([q_0], a_0)\lambda_2^*(\delta_2([q_0], a_0), a_1 \cdots a_k) \\
&= \lambda_1(q_0, a_0)\lambda_2^*([\delta_1(q_0, a_0)], a_1 \cdots a_k) \\
&= \lambda_1(q_0, a_0)\lambda_1^*(\delta_1(q_0, a_0), a_1 \cdots a_k).
\end{aligned}$$

由归纳法, $\forall w \in \Sigma^*$, 有 $\lambda_1^*(q_0, w) = \lambda_2^*([q_0], w)$. ∎

能否对有穷自动机进行化简得到一个等价的简化自动机呢? 这是可以做到的.

定义 2.11 设 $M = \langle Q, \Sigma, \Gamma, \delta, \lambda\rangle$ 是有穷自动机, $\sim$ 是定义 2.8 中的等价关系, 若 $\sim$ 是恒等关系, 则称 M 是一个**极小的有穷自**

动机.

可以证明对任意有穷自动机 M 都存在一个等价的极小有穷自动机. 在定义了有穷自动机的同构以后,在同构的意义下这个等价的极小有穷自动机是唯一的,就是它的商自动机. 作为独异点的重要应用,我们引入了有穷自动机的相关概念. 限于篇幅,这里不再讨论化简有穷自动机的算法. 有兴趣的读者可以阅读有关自动机理论的书籍.

习　题　二

1. 在 R 中定义二元运算$\circ$,

$$a\circ b = a + b + ab, \ \forall a,b \in R.$$

证明

(1) $\langle R,\circ\rangle$ 是半群;

(2) $\langle R,\circ\rangle$ 是独异点.

2. 设 $V = \langle S, * \rangle$ 是半群,若存在 $a \in S$ 使得对任意的 $x \in S$ 有 $u,v \in S$ 满足

$$a * u = v * a = x,$$

证明 V 是独异点.

3. $S = \{a,b,c\}$,$\circ$是 S 上的二元运算且

$$x\circ y = x, \quad \forall x,y \in S.$$

(1) 证明$\langle S,\circ\rangle$ 是半群;

(2) 将$\langle S,\circ\rangle$ 扩充为一个独异点.

4. $V = \langle S,\circ\rangle$ 是半群,$a,b,c \in S$. 若 a 和 c 是可交换的,b 和 c 也是可交换的,证明 $a\circ b$ 与 c 也是可交换的.

5. 设 $V = \langle \{a,b\}, * \rangle$ 是半群,且 $a * a = b$. 证明

(1) $a * b = b * a$;

(2) $b * b = b$.

6. 设 $V = \langle S,\circ\rangle$ 是半群,任取 $a,b \in S, a \neq b$,则有 $a\circ b \neq b\circ a$. 证明

(1) $\forall a \in S$ 有 $a\circ a = a$;

(2) $\forall a,b \in S$ 有 $a\circ b\circ a = a$;

(3) $\forall a,b,c \in S$ 有 $a\circ b\circ c = a\circ c$.

7. 设 $V=\langle S,*\rangle$ 是可交换半群，若 $a,b\in S$ 是 V 中的幂等元，证明 $a*b$ 也是 V 中的幂等元.

8. 设 $V=\langle S,\circ\rangle$ 是半群，$\theta_l\in S$ 是一个左零元，证明 $\forall x\in S$，$x\circ\theta_l$ 也是一个左零元.

9. 证明每个有限半群都存在幂等元.

10. $V=\langle Z_4,\otimes\rangle$，其中 $\otimes$ 表示模 4 乘法. 找出 V 的所有子半群. 并说明哪些子半群是 V 的子独异点.

11. $V=\langle A,*\rangle$ 是半群，其中 $A=\{a,b,c,d\}$，$*$ 运算由表 2.4 给定，$\sim$ 为 A 上的同余关系，且同余类是

$[a]=[c]$，　$[b]=[d]$.

试给出商代数 $V/\sim$ 的运算表.

表 2.4

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

12. $V=\langle S,\circ\rangle$ 是半群，I 是 S 的非空子集，且满足 $IS\subseteq I$ 和 $SI\subseteq I$，其中 $IS=\{a\circ x\mid a\in I\wedge x\in S\}$，$SI=\{x\circ a\mid x\in S\wedge a\in I\}$. 称 I 是 V 的理想. 在 S 上定义二元关系 R，

$$xRy\Leftrightarrow x=y\vee(x\in I\wedge y\in I).$$

(1) 证明 R 是 V 上的同余的关系；

(2) 描述商代数 $\langle S/R,\bar{\circ}\rangle$.

13. IR 触发器有两个状态：0 和 1. 当输入“0”时，不管触发器原有状态是什么，触发器状态都要置 0，并将触发器的原状态输出. 当输入为“1”时，不管触发器的原状态而将触发器置 1，并将触发器的原状态输出. 当输入为“e”时，触发器状态不变，只是将触发器状态输出. 试用有穷自动机 $M=\langle Q,\Sigma,\Gamma,\delta,\lambda\rangle$ 来描述 IR 触发器. 确定 $Q,\Sigma,\Gamma,\delta,\lambda$，并画出图.

14. 设有穷自动机 $M=\langle Q,\Sigma,\Gamma,\delta,\lambda\rangle$ 如图 2.2 所示. 每条有向边上括号内的字符是输出字符. 试确定 Q,Σ,Γ，并给出 δ,λ 的函数表.

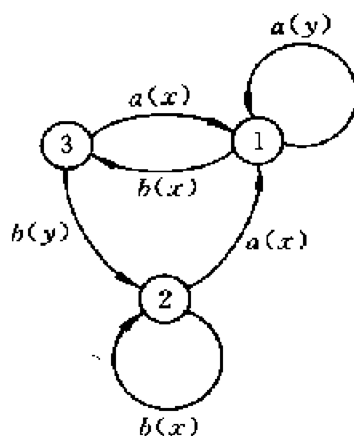


图 2.2

15. $Q=\{0,1,\cdots,4\}$，$\Sigma=Q$，$\delta: Q\times\Sigma\to Q$ 定义如下：

$$\forall q\in Q, a\in\Sigma, \delta(q,a)=q\oplus a, \oplus \text{ 为模 5 加.}$$

给出半自动机 $M=\langle Q,\Sigma,\delta\rangle$ 的转移函数表和图.

16. 设 $M=\langle Q,\Sigma,\Gamma,\delta,\lambda\rangle$ 是有穷自动机，其中 $Q=\{q_0,q_1,\cdots,q_6\}$，$\Sigma=\{0,1\}$，$\Gamma=\{0,1\}$，δ,λ 如表 2.5 所示. 试确定 M 的商自动机 $\overline{M}=\langle Q/\sim,\Sigma,\Gamma,\overline{\delta},\overline{\lambda}\rangle$.

表 2.5

δ	0	1
q_0	q_1	q_6
q_1	q_1	q_6
q_2	q_4	q_0
q_3	q_5	q_1
q_4	q_4	q_2
q_5	q_5	q_3
q_6	q_0	q_5

λ	0	1
q_0	0	0
q_1	0	0
q_2	0	0
q_3	0	0
q_4	1	0
q_5	1	0
q_6	0	1

第三章　群

§3.1　群的定义和性质

群是一类很重要的代数系统. 在许多领域都有着广泛的应用.

定义 3.1　$\langle G, \circ\rangle$ 是含有一个二元运算的代数系统，如果满足以下条件：

(1) $\circ$ 运算是可结合的，

(2) 存在 $e \in G$ 是关于 $\circ$ 运算的单位元，

(3) 任何 $x \in G$，x 关于 $\circ$ 运算的逆元 $x^{-1} \in G$，

则称 G 是一个群.

【例 3.1】

(1) $\langle Z, +\rangle$ 是一个群，称为**整数加群**. 其中 0 是单位元，$\forall x \in Z$，$-x$ 是 x 的逆元.

(2) $\langle Z_n, \oplus\rangle$ 是群，称为**模 n 整数加群**，其中 $Z_n = \{0,1,\cdots,n-1\}$，$x \oplus y = (x+y)\bmod n$，$\forall x, y \in Z_n$.

(3) 设 $n \geqslant 2$，$\langle M_n(R), +\rangle$ 是群，称为 **n 阶实矩阵加群**. n 阶全零矩阵是单位元，$-M$ 是矩阵 M 的加法逆元.

(4) $\langle P(B), \oplus\rangle$ 是群，其中 $P(B)$ 是集合 B 的幂集，$\oplus$ 为集合的对称差运算. $\varnothing$ 是单位元，$\forall B' \in P(B)$，B' 就是它自己的逆元.

(5) 设 S 是 A^A 中所有双射函数的集合，则 S 关于函数的合成运算构成一个群. A 上的恒等函数 I_A 是单位元，f^{-1} 是 f 的逆元.

【例 3.2】　令 $G = \{e, a, b, c\}$，$\circ$ 运算由表 3.1 给出. 容易验证 $\circ$ 运算是可结合的，e 是 G 中的单位元，$\forall x \in G$，$x^{-1} = x$. G 关于 $\circ$ 运算构成一个群，称为 **Klein 四元群**.

表 3.1

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

定理 3.1 设$\langle G,\circ\rangle$是具有一个可结合二元运算的代数系统. 若存在$e\in G$,使得$\forall a\in G$有$a\circ e=a$,且$\forall a\in G$,存在$a'\in G$满足$a\circ a'=e$,则G是一个群.

证 先证e也是G中的左单位元.

$\forall a\in G$有$a\circ e=a$,所以有$e\circ e=e$. 由题设存在$a'\in G$使得$a\circ a'=e$. 将$a\circ a'$代入上式得

$$e\circ(a\circ a')=a\circ a'.$$

因为$a'\in G$,存在$a''\in G$,使得$a'\circ a''=e$. 上式两边右乘a''得

$$e\circ a\circ a'\circ a''=a\circ a'\circ a'',$$

而$a'\circ a''=e$,因此有$e\circ a=a$. e是G中的单位元.

再证$\forall a\in G$,a'也是a的左逆元,我们只须证明$a''=a$即可.

$$a''=e\circ a''=(a\circ a')\circ a''=a\circ(a'\circ a'')=a\circ e=a. \quad ∎$$

定理 3.1 可以做为群的等价定义来使用. 类似地可以证明:对于具有一个可结合的二元运算的代数系统,若存在左单位元e,且相对于这个左单位元每个元素都有左逆元,则这个代数系统也是群.

下面介绍和群有关的一些概念.

定义 3.2 (1) 若群G中只含有一个元素,即$G=\{e\}$,则称G为**平凡群**.

(2) 若群G中运算满足交换律,则称G为**交换群**或**Abel 群**. .

例如$\langle\{0\},+\rangle$是平凡群. 整数加群$\langle Z,+\rangle$和模n整数加群$\langle Z_n,\oplus\rangle$是 Abel 群,Klein 四元群也是 Abel 群.

定义 3.3 群G的基数称为群G的**阶**,若群G的阶是正整数n,称G为n阶群,记作$|G|=n$,否则称G为**无限群**.

整数加群是无限群,模n整数加群是n阶群,Klein 四元群是 4 阶群.

定义 3.4 G是群,$a\in G$, a的n**次幂**$(n\in Z)$

$$a^n = \begin{cases} e, & n = 0; \\ a^{n-1}a, & n > 0; \\ (a^{-1})^m, & n = -m, m > 0. \end{cases}$$

例如 Klein 四元群$\{e,a,b,c\}$中,$a^0 = e$, $a^1 = a$, $a^2 = e$,$a^{-1} = a$,$a^{-2} = a^2 = e$ 等等.

定义 3.5　G是群,$a \in G$,使得$a^k = e$成立的最小正整数k称为a的**阶**,记作$|a|$.

【例 3.3】

(1) 整数加群$\langle Z, +\rangle$中$|0| = 1$,其它元素的阶不存在.模 6 整数加群$\langle Z_6, \oplus\rangle$中,$|0| = 1$,$|1| = |5| = 6$,$|2| = |4| = 3$,$|3| = 2$.

(2) Klein 四元群$\{e,a,b,c\}$中e是 1 阶元,a,b和c都是 2 阶元.

下面讨论群的性质.

定理 3.2　G为群,$\forall a,b \in G$有

(1) $(a^{-1})^{-1} = a$;

(2) $(ab)^{-1} = b^{-1}a^{-1}$;

(3) $a^n a^m = a^{n+m}$,　　　$m,n \in Z$;

(4) $(a^n)^m = a^{nm}$,　　　$m,n \in Z$;

(5) 若G为 Abel 群,$(ab)^n = a^n b^n$,　$n \in Z$.

证　只证(1)和(3),其它的留作练习.

(1) $\forall a \in G$,a是a^{-1}的逆元,由逆元的唯一性得$(a^{-1})^{-1} = a$.

(3) 当$m,n \in N$时,根据独异点中幂运算的规则有$a^n a^m = a^{n+m}$.下面对n或m小于 0 的情况进行验证. 不妨设$n < 0$, $m \geq 0$,则$n = -n_1$,$n_1 > 0$.

$$a^n a^m = a^{-n_1} a^m = \underbrace{a^{-1}\cdots a^{-1}}_{n_1\text{个}}\underbrace{a\cdots a}_{m\text{个}}$$

$$= \begin{cases} a^{m-n_1} & m \geq n_1 \\ (a^{-1})^{n_1-m} & m < n_1 \end{cases}$$

$$= a^{m+n}.$$

对于其它的情况也可以类似地得到验证. ∎

定理 3.2 中的等式 $(ab)^{-1}=b^{-1}a^{-1}$ 可以推广到 k 个元素的情况，即 $\forall a_1,a_2,\cdots,a_k\in G$ 有

$$(a_1a_2\cdots a_k)^{-1}=a_k^{-1}\cdots a_2^{-1}a_1^{-1}.$$

不难使用数学归纳法对这个等式加以证明.

定理 3.3　G 为群，$\forall a,b\in G$，方程 $ax=b$ 和 $ya=b$ 在 G 中有解且有唯一解.

证　$\forall a,b\in G$ 有 $a(a^{-1}b)=(aa^{-1})b=b$，所以 $a^{-1}b$ 是方程 $ax=b$ 的一个解.

假设 c 是方程 $ax=b$ 的解，则有

$$c=ec=(a^{-1}a)c=a^{-1}(ac)=a^{-1}b.$$

这就证明了 $a^{-1}b$ 是方程 $ax=b$ 的唯一解.

同理可证 ba^{-1} 是方程 $ya=b$ 的唯一解. ∎

以上定理给出了群的性质，反过来，我们也可以利用这条性质来定义群.

定理 3.4　设 G 是具有一个可结合的二元运算的代数系统，如果 $\forall a,b\in G$ 方程 $ax=b$ 和 $ya=b$ 在 G 中有解，则 G 是群.

证　任取 G 中一个元素 b，方程 $bx=b$ 在 G 中有解，将这个解记作 e.

$\forall a\in G$，方程 $yb=a$ 在 G 中有解，将这个解记作 c，即 $cb=a$. 那么有

$$ae=(cb)e=c(be)=cb=a,$$

e 是 G 中的右单位元.

$\forall a\in G$，方程 $ax=e$ 在 G 中有解，恰为 a 相对于 e 的右逆元. 由定理 3.1，G 是一个群. ∎

定理 3.5　群中运算满足消去律.

证　$\forall a,b,c\in G$，

$$ab=ac\Rightarrow a^{-1}(ab)=a^{-1}(ac)\Rightarrow b=c;$$

同理可证　$ba = ca \Rightarrow b = c$. ∎

这条性质也可以用来定义群. 请看下面的定理.

定理 3.6　设 G 是具有一个二元运算的不含零元的有限代数系统, 且该运算适合结合律和消去律, 则 G 是一个群.

证　令 $G = \{a_1, a_2, \cdots, a_n\}$. $\forall a, b \in G$, 令

$$aG = \{aa_i \mid i = 1, 2, \cdots, n\},$$

则 $aG \subseteq G$, 且 aG 中元素两两不同. 若不然有 $aa_j = aa_l$, 由消去律可得 $a_j = a_l$, 与 G 中有 n 个元素矛盾. 因此 aG 中含有 n 个元素. 由 $aG = G$, 必存在 $a_i \in G$, 使得 $aa_i = b$, 方程 $ax = b$ 在 G 中有解.

同理可证方程 $ya = b$ 在 G 中也有解, 根据定理 3.4, G 是群.

∎

定理 3.7　设 $G = \{a_1, a_2, \cdots, a_n\}$ 为群, 则 G 的运算表的每行每列都是 G 中元素的一个置换.

证　对任意的 $i = 1, 2, \cdots, n$, 设 $a_{i1}, a_{i2}, \cdots, a_{in}$ 是运算表的第 i 行, 假设 $a_{ij} = a_{il}$, 根据运算表的定义有 $a_i a_j = a_i a_l$. 由于群中运算满足消去律, 因此有 $a_j = a_l$, 与 G 中有 n 个元素矛盾. 这就证明 G 中任何元素在运算表的一行中至多出现一次.

任取 $a_j \in G$(对于 $i = 1, 2, \cdots, n$) 方程 $a_i x = a_j$ 在 G 中有解. 若 $x = a_k$, 则 a_j 出现在第 i 行第 k 列上. 因此 a_j 在运算表的每一行中至少出现一次.

综上所述, 运算表的每一行是 G 中元素的一个置换, 同理可证运算表的每一列也是 G 中的元素一个置换. ∎

定理 3.8　G 是群, $a \in G$ 且 $|a| = r$, 则

(1) $a^k = e$ 当且仅当 $r \mid k$, $k \in Z$,

(2) $|a| = |a^{-1}|$,

(3) 若 $|G| = n$, 则 $r \leqslant n$.

证　(1) 充分性. 已知 $r \mid k$, 即存在整数 l, 使得 $k = lr$. 所以有

$$a^k = a^{lr} = (a^r)^l = e^l = e.$$

必要性. 根据除法有 $k = lr + i$,其中 $l \in Z, i \in \{0,1,\cdots,r-1\}$,因为 $a^k = e$,所以有

$$e = a^k = a^{lr+i} = (a^r)^l \cdot a^i = a^i,$$

a 的阶是 r,且 $i < r$,因此 $i = 0$. 这就证明了 $r|k$.

(2) 由

$$(a^{-1})^r = a^{-r} = (a^r)^{-1} = e$$

可知 a^{-1} 的阶存在,令 $|a^{-1}| = t$,则 $t|r$,而 a 也是$(a^{-1})^{-1}$,所以有 $r|t$. 这就证明了 $r = t$.

(3) 假设 $r > n$,则 $e,a,a^2,\cdots,a^{r-1}$ 必两两不同. 若不然有 $a^i = a^j, 0 \leqslant i < j \leqslant r-1$. 由消去律得 $a^{j-i} = e$,与 $|a| = r$ 矛盾. 令 $G' = \{e,a,a^2,\cdots,a^{r-1}\}$,则 $|G'| = r > |G|$,与 $G' \subseteq G$ 矛盾. ∎

以上给出了群的五条重要的性质. 下面的例子说明了这些性质的应用.

【例 3.4】 证明单位元 e 是群 G 中唯一的幂等元.

证 易见 e 是 G 中的幂等元. 假设 x 也是 G 中的幂等元,则有 $x^2 = x$,由消去律可得 $x = e$. ∎

【例 3.5】 G 是群,若 $\forall x \in G$ 都有 $x^2 = e$,证明 G 是 Abel 群.

证 $\forall x,y \in G$,有

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$

所以 G 是 Abel 群 ∎

【例 3.6】 G 为群,$a,b \in G$ 是可交换的元素,且 $|a| = n, |b| = m$. 若$(n,m) = 1$,则 $|ab| = nm$.

证 设 $|ab| = d$,

$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e,$$

所以 $d|nm$. 又由$(ab)^d = e$ 得 $a^d b^d = e$,即有 $a^d = b^{-d}$. 由定理 3.8 得 $|a^d| = |b^d|$. 由于

$$(a^d)^n = (a^n)^d = e,$$

因此有 $|a^d|\,|n$. 同理有 $|b^d|\,|m$. 从而推出

$$|a^d| \mid (n,m).$$

已知$(n,m)=1$,所以$|a^d|=1$.这说明$a^d=e$,同时$b^d=e$.根据定理3.8有$n \mid d$和$m \mid d$,因此$[n,m]$①$\mid d$,即$nm \mid d$,从而证明了

$$|ab| = d = nm. \qquad \blacksquare$$

【例3.7】 设a,b是群G中可交换的元素,$|a|=n$,$|b|=m$,证明G中存在元素c使得$|c|=[n,m]$.

证 若$n \mid m$或$m \mid n$,则c就是b或a.我们考虑$n \nmid m$,$m \nmid n$的情况.将n,m作质因数分解如下:

$$n = p_1^{t_1} p_2^{t_2} \cdots p_i^{t_i} p_{i+1}^{t_{i+1}} \cdots p_l^{t_l},$$

$$m = p_1^{s_1} p_2^{s_2} \cdots p_i^{s_i} p_{i+1}^{s_{i+1}} \cdots p_l^{s_l}.$$

其中$p_1,\cdots,p_l$为质数,$t_1,\cdots,t_l,s_1,\cdots,s_l$为非负整数.适当排列质因子的顺序使得$t_1 \geqslant s_1$, $t_2 \geqslant s_2$, $\cdots$, $t_i \geqslant s_i$, $t_{i+1} < s_{i+1}$, $\cdots$, $t_l < s_l$.易见

$$(n,m) = p_1^{s_1} \cdots p_i^{s_i} p_{i+1}^{t_{i+1}} \cdots p_l^{t_l},$$

$$[n,m] = p_1^{t_1} \cdots p_i^{t_i} p_{i+1}^{s_{i+1}} \cdots p_l^{s_l}.$$

令$x = a^{p_{i+1}^{t_{i+1}} \cdots p_l^{t_l}}$, $y = b^{p_1^{s_1} \cdots p_i^{s_i}}$,则$|x| = p_1^{t_1} \cdots p_i^{t_i}$, $|y| = p_{i+1}^{s_{i+1}} \cdots p_l^{s_l}$.因为$p_1,\cdots,p_l$是各不相同的质数,所以$(|x|,|y|)=1$.由例3.6,$xy$的阶是$|x| \cdot |y| = p_1^{t_1} \cdots p_i^{t_i} p_{i+1}^{s_{i+1}} \cdots p_l^{s_l} = [n,m]$. $\blacksquare$

§3.2 子群

定义3.6 G是群,H是G的非空子集,若H关于G中的运算构成一个群,则称H是G的**子群**,记作$H \leqslant G$.如果子群H是G的真子集,则称H是G的**真子群**,记作$H < G$.

【例3.8】 (1) $\langle Z, +\rangle$是$\langle Q, +\rangle$,$\langle R, +\rangle$的子群,$\langle Q, +\rangle$是$\langle R, +\rangle$的子群.$\langle \{0\}, +\rangle$和$\langle R, +\rangle$都是$\langle R, +\rangle$的子群.

---

① $[n,m]$表示n和m的最小公倍数.

(2) $G=\langle Z,+\rangle$ 是整数加群，则对任意的 $n\in N$，$nZ=\{nk\mid k\in Z\}$ 都是 G 的子群，且任何 G 的子群都具有 nZ 的形式. 下面给出证明.

任取 $nk_1,nk_2\in nZ$，有 $nk_1+nk_2=n(k_1+k_2)\in nZ$. $0=n\cdot 0\in nZ$ 是 nZ 中的单位元. $\forall nk\in nZ$，$-nk=n(-k)\in nZ$ 是 nk 的逆元. 因此 nZ 关于 G 中的加法构成群，是 G 的子群.

设 H 是 G 的任一子群. 若 $H=\{0\}$，则 $H=0Z,0\in N$；否则存在 $a\in H,a\neq 0$. 取 H 中最小的正整数，记作 n，则 $nZ\subseteq H$. 任取 H 中的元素 b，根据除法有 $b=nl+r$，其中 $l,r\in Z$ 且 $0\leqslant r<n$. 由于 $H\leqslant G$，所以 $r=b-nl=b+(-nl)\in H$. 从而有 $r=0$，否则与 n 是 H 中的最小正整数矛盾. 于是 $b=nl\in nZ$，这就推出 $H\subseteq nZ$. 综合上述，$H=nZ$.

G 是群，$H\leqslant G$，如果 $H=\{e\}$ 或 $H=G$，则称 H 是 G 的**平凡子群**. 考虑 $\langle Z,+\rangle$ 的子群 nZ，当 $n=0$ 时，$\{0\}$ 是 $\langle Z,+\rangle$ 的平凡子群，也是真子群. 当 $n=1$ 时，$nZ=Z$ 是 $\langle Z,+\rangle$ 的另一个平凡子群. 除此之外，nZ 都是 $\langle Z,+\rangle$ 的非平凡的真子群.

如果把群看作代数系统 $\langle G,\circ,^{-1},e\rangle$，其中 e 是 G 中关于 $\circ$ 运算的单位元，是该代数系统的零元运算. $\forall x\in G$，x^{-1} 是 x 的逆元，求逆运算 $^{-1}$ 是 G 中的一元运算. 可以证明 G 的子群就是代数系统 $\langle G,\circ,^{-1},e\rangle$ 的子代数.

设 $H\leqslant G$，我们只需验证：H 中的单位元 e' 就是 G 中的单位元 e，且 $\forall x\in H$，x 在 H 中的逆元 x' 就是 x 在 G 中的逆元 x^{-1}. 任取 $x\in H$，有 $x\circ e'=x=x\circ e$，由 G 中的消去律得 $e'=e$. 再由 $x\circ x'=e'=e=x\circ x^{-1}$ 得到 $x'=x^{-1}$.

群 G 的子群是 G 的子代数. 而对于独异点 $V=\langle S,\cdot,e\rangle$，尽管 S 的子集 B 可以关于 V 中的 $\cdot$ 运算构成一个独异点 $\langle B,\cdot,e'\rangle$，但不一定是 V 的子独异点，因为可能 $e'\neq e$.

下面给出子群的判定定理.

定理 3.9　G是群,H是G的非空子集,则H是G的子群当且仅当

(1) $\forall a,b \in H$ 有 $ab \in H$,

(2) $\forall a \in H$ 有 $a^{-1} \in H$.

证　必要性是显然的,下面证明充分性.我们只需证明 $e \in H$ 即可.H 非空,存在 $a \in H$.由(2)有 $a^{-1} \in H$.再由 $a \in H$ 和 $a^{-1} \in H$,根据(1)有 $aa^{-1} = e \in H$. ∎

定理 3.10　G是群,H是G的非空子集,则H是G的子群当且仅当 $\forall a,b \in H$ 有 $ab^{-1} \in H$.

证　必要性是显然的,只证充分性.由H非空必存在$b \in H$.根据已知条件则有 $bb^{-1} \in H$,即 $e \in H$,任取 $a \in H$,由 $e \in H$ 且 $a \in H$,则有 $ea^{-1} = a^{-1} \in H$.任取 $a,b \in H$,根据上面的证明有 $b^{-1} \in H$.再使用已知条件有 $a(b^{-1})^{-1} \in H$,即 $ab \in G$,所以H是G子群. ∎

定理 3.11　G是群,H是G的有穷非空子集,则H是G的子群当且仅当 $\forall a,b \in H$ 有 $ab \in H$.

证　必要性是显然的.为证明充分性,根据定理 3.9 只需证明 $\forall a \in H$ 有 $a^{-1} \in H$ 即可.

$\forall a \in H$,若 $a = e$,则 $a^{-1} = a$.设 $a \neq e$,令

$$S = \{a, a^2, \cdots, a^k, \cdots\},$$

则 $S \subseteq H$.由于H是有穷集,必存在 $a^i = a^j (i < j)$.由消去律得 $a^{j-i} = e$.因为 $a \neq e$,所以 $j - i \neq 1$,即 $j - i - 1 > 0$.故 $e = a^{j-i-1}a$,$a^{-1} = a^{j-i-1} \in H$. ∎

以上三个判定定理分别称作子群判定定理一、二和三.请看下面的例子.

【例 3.9】　G是群,$a \in G$,令

$$\langle a \rangle = \{a^k \mid k \in Z\},$$

则$\langle a \rangle$是G的子群,叫做**由 a 生成的子群**.

证 $a \in \langle a \rangle$，所以$\langle a \rangle$是G的非空子集. 任取$a^i, a^j \in \langle a \rangle, i, j \in Z$，有

$$a^i(a^j)^{-1} = a^{i-j} \in \langle a \rangle.$$

由判定定理二有$\langle a \rangle \leqslant G$. ∎

例如$G = \langle Z_6, \oplus \rangle$，则$\langle 1 \rangle = \langle 5 \rangle = Z_6$，$\langle 2 \rangle = \langle 4 \rangle = \{0,2,4\}$，$\langle 3 \rangle = \{0,3\}$，$\langle 0 \rangle = \{0\}$.

【例 3.10】 G 是群，令

$$C = \{a \mid a \in G \text{ 且 } \forall x \in G(ax = xa)\},$$

则 C 是 G 的子群，称作 G 的**中心**.

证 $\forall x \in G(ex = xe)$，即 $e \in C$，C 非空. 任取 $a, b \in C$，$\forall x \in G$ 有

$$(ab^{-1})x = ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1}$$
$$= a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}).$$

所以 $ab^{-1} \in C$. 由判定定理二有 $C \leqslant G$. ∎

易见当 G 是 Abel 群时有 $C = G$，如果群 G 的中心为$\{e\}$，则称 G 是无中心的.

【例 3.11】 G 是群，H 是 G 的子群，$x \in G$，令

$$xHx^{-1} = \{xhx^{-1} \mid h \in H\},$$

则 xHx^{-1} 是 G 的子群，称为 H 的**共轭子群**.

证 $e = xex^{-1} \in xHx^{-1}$，$xHx^{-1}$ 非空. 任取 $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$，有

$$(xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}.$$

由判定定理二有 $xHx^{-1} \leqslant G$. ∎

【例 3.12】 G 是群，H 和 K 是 G 的子群，则

(1) $H \cap K \leqslant G$，

(2) $H \cup K \leqslant G$ 当且仅当 $H \subseteq K$ 或 $K \subseteq H$.

证 (1) $e \in H \cap K$，$H \cap K$ 非空. 任取 $a, b \in H \cap K$，则 $a \in H$，$a \in K$，$b \in H$，$b \in K$. 又由于 H 和 K 是 G 的子群，所以 $b^{-1} \in H$，

$b^{-1} \in K$. 这就得到 $ab^{-1} \in H$ 和 $ab^{-1} \in K$，即 $ab^{-1} \in H \cap K$. 由判定定理二有 $H \cap K \leqslant G$.

(2) 充分性是显然的，只证必要性. 假设 $H \nsubseteq K$ 且 $K \nsubseteq H$，则存在 $h \in H$ 且 $h \notin K$，同时存在 $k \in K$ 且 $k \notin H$. 如果 $hk \in H$，则 $k = h^{-1} \cdot hk \in H$，与假设矛盾，所以 $hk \notin H$. 同理可证 $hk \notin K$. 因此 $hk \notin H \cup K$，而 $h,k \in H \cup K$，与 $H \cup K \leqslant G$ 矛盾. ∎

【例 3.13】 G 是群，B 是 G 的非空子集，令

$$S = \{H \mid H \leqslant G \text{ 且 } B \subseteq H\},$$

则 S 非空，设 $K = \bigcap S$，则 K 是 G 的子群，称为**由 B 生成的子群**，记作 $\langle B \rangle$.

证 $e \in K$，K 非空，任取 $x,y \in K$，则 x 和 y 属于 G 的每一个包含 B 的子群 H，因此 $xy^{-1} \in H$. 根据 H 的任意性，有 $xy^{-1} \in K$. 由判定定理二得 $K \leqslant G$. ∎

由 $\langle B \rangle$ 的定义可知，$\langle B \rangle$ 中的元素是 B 中元素或它们的逆元构成的有限序列. 即

$$\langle B \rangle = \{a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n} \mid n \in Z^+ \text{ 且 } i = 1,2,\cdots,n, a_i \in B, e_i = \pm 1\}.$$

例如 $G = \langle Z, + \rangle$ 是整数加群，$B_1 = \{2,3\}$，$B_2 = \{2\}$，则 $\langle B_1 \rangle = G$，$\langle B_2 \rangle = 2Z$.

定义 3.7 G 是群，S 是 G 的所有子群的集合，在 S 上定义二元关系 R，$\forall H_1, H_2 \in S$ 有

$$H_1 R H_2 \Leftrightarrow H_1 \leqslant H_2.$$

不难证明 R 是 S 上的偏序关系并且 S 关于 R 构成一个格，称为 G 的**子群格**（见第五章格的定义）.

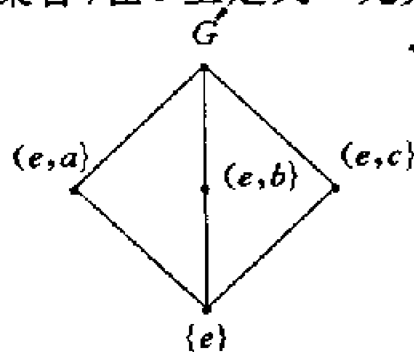


图 3.1

【例 3.14】 $G = \{e,a,b,c\}$ 是 Klein 四元群，G 的子群是：$\{e\}$，$\{e,a\}$，$\{e,b\}$，$\{e,c\}$ 和 G，G 的子群格的哈斯图如图 3.1 所示.

【例 3.15】 $G = \langle Z_{12}, \oplus \rangle$ 为模 12 整数加群，G 有六个子群：

$$H_1 = \{0\} = \langle 0 \rangle,$$
$$H_2 = \{0,6\} = \langle 6 \rangle,$$
$$H_3 = \{0,4,8\} = \langle 4 \rangle,$$
$$H_4 = \{0,3,6,9\} = \langle 3 \rangle,$$
$$H_5 = \{0,2,4,6,8,10\} = \langle 2 \rangle,$$
$$G = Z_{12}.$$

G 的子群格如图 3.2 所示.

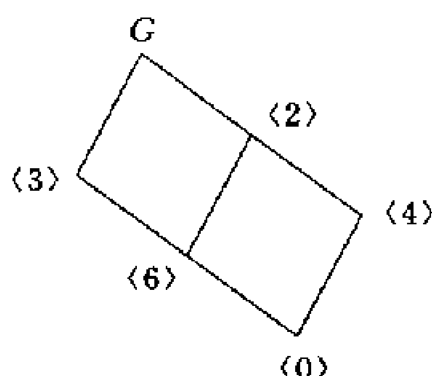


图 3.2

§3.3 循环群

循环群是一类重要的群.

定义 3.8 G 是群,若存在 $a \in G$ 使得

$$G = \{a^k \mid k \in Z\},$$

则称 G 为**循环群**,记作 $\langle a \rangle$,称 a 是 G 的**生成元**.

在循环群 $\langle a \rangle$ 中,若 $|a| = n$,则 $\langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$,叫做 n 阶循环群. 若 $|a|$ 不存在,则 $\langle a \rangle = \{e, a, a^{-1}, a^2, a^{-2}, \cdots\}$ 也是无限的,称为**无限阶循环群**. 例如整数加群 $\langle Z, + \rangle$ 是无限阶循环群,1 是它的一个生成元. 而模 n 整数加群 $\langle Z_n, \oplus \rangle$ 是 n 阶循环群,1 也是它的一个生成元.

下面考虑循环群的生成元. 先给出**欧拉函数** $\phi(n)$ 的定义. 设 n 是正整数,欧拉函数 $\phi(n)$ 是小于等于 n 且与 n 互质的正整数个数.

例如 $n = 12$,小于等于 12 且与 12 互质的正整数是 1,5,7 和 11,因此 $\phi(12) = 4$.

定理 3.12 $G = \langle a \rangle$ 是循环群.

(1) 若 G 是无限阶循环群,则 G 的生成元是 a 和 a^{-1}.

(2) 若 G 是 n 阶循环群,则 G 有 $\phi(n)$ 个生成元. 当 $n = 1$ 时,$G = \langle e \rangle$ 的生成元是 e,当 $n > 1$ 时,对于每一个小于等于 n 的正整数 r,a^r 是 G 的生成元当且仅当 $(n, r) = 1$.

证 (1) $G = \langle a \rangle$ 是无限阶循环群,a 是 G 的一个生成元. 任取 a^i

$\in \langle a \rangle, a^i = (a^{-1})^{-i}$,即 a^i 可以表成 a^{-1} 的整数次幂,所以 a^{-1} 也是 G 的一个生成元. 设 $b \in \langle a \rangle$ 是 G 的生成元,不妨设 $b = a^j$. 由于 b 是 $\langle a \rangle$ 的生成元,a 也可以用 b 的幂表出,即存在整数 t,使得 $a = b^t = (a^j)^t = a^{jt}$. 由消去律得 $a^{jt-1} = e$. 注意到 a 是无限阶元,则有 $jt - 1 = 0$. 而 j,t 都是整数,从而有 $j = t = 1$ 或 $j = t = -1$. 这就证明了 G 中只有 a 或 a^{-1} 是生成元.

(2) $n = 1$ 时结论显然为真,不妨设 $n \geqslant 2$. 先证充分性. 若 $(r,n) = 1$,则存在整数 u,v 使得

$$ur + vn = 1,$$

于是有

$$a = a^{ur+vn} = a^{ur}a^{vn} = (a^r)^u(a^n)^v = (a^r)^u.$$

因此任何 $a^i \in \langle a \rangle$,都有 $a^i = (a^r)^{ui}$,即 a^i 可以用 a^r 的整数次幂表示,a^r 是 G 的生成元.

再证必要性. 若 a^r 是 G 的生成元,设 $(r,n) = d$,即存在非零整数 t 使得 $r = dt$. 由于

$$(a^r)^{\frac{n}{d}} = (a^{dt})^{\frac{n}{d}} = a^{tn} = (a^n)^t = e^t = e,$$

所以由定理 3.8 可知 a^r 的阶是 $\frac{n}{d}$ 的因子. 而 a^r 是 n 阶循环群的生成元,故 a^r 的阶是 n,这就推出 n 是 $\frac{n}{d}$ 的因子. 从而必有 $d = 1$,即 r 与 n 互质. ▮

例如 $G = \langle a \rangle$ 是 12 阶循环群,$\phi(12) = 4$,与 12 互质的数有 1,5,7 和 11. 由定理 3.12, a,a^5,a^7 和 a^{11} 都是 G 的生成元.

下面讨论循环群的子群.

定理 3.13 $G = \langle a \rangle$ 是循环群,那么

(1) G 的子群也是循环群.

(2) 若 G 是无限阶的,则 G 的子群除 $\{e\}$ 以外仍是无限阶的.

(3) 若 G 是 n 阶的,则 G 的子群的阶是 n 的因子,对于 n 的每个

正因子 d，在 G 中有且仅有一个 d 阶子群.

证 (1) 设 H 是 $G=\langle a\rangle$ 的子群. 如果 $H=\{e\}$，则 H 是循环群，否则取 H 中最小正方幂元 a^m. 对于 H 中的任一元素 a^i，根据除法有 $i=lm+r$, $l,r\in Z$，且 $0\leqslant r<m$，因此

$$a^r=a^i(a^m)^{-l}\in H.$$

这就推出 $r=0$，否则与 a^m 是 H 中最小正方幂元矛盾. $a^i=(a^m)^l$，即 a^i 可由 a^m 的幂表出，a^m 是 H 的生成元，因此 $H=\langle a^m\rangle$.

(2) G 是无限阶循环群，H 是 G 的子群. 若 $H\neq\{e\}$，由于 H 是循环群，必有 $H=\langle a^m\rangle$，$a^m\neq e$. 假若 $|H|=t$，则 $(a^m)^t=e$，即 $a^{mt}=e$，与 a 是无限阶元矛盾.

(3) $G=\{e,a,a^2,\cdots,a^{n-1}\}$ 是 n 阶循环群. H 是 G 的子群，不妨设 $H\neq\{e\}$. 根据(1) 有 $H=\langle a^m\rangle$，设 $|a^m|=d$，则有

$$(a^m)^n=(a^n)^m=e^m=e.$$

由定理 3.8 知 $d|n$.

设 d 是 n 的正因子，易见 $H=\langle a^{\frac{n}{d}}\rangle$ 是 G 的 d 阶子群. 假若 $H_1=\langle a^m\rangle$ 也是 G 的 d 阶子群，其中 a^m 是 H_1 中的最小正方幂元. 由于 a^m 的阶是 d，

$$a^{md}=(a^m)^d=e.$$

根据定理 3.8 得 $n|md$，即 $\left.\frac{n}{d}\right|m$. 令 $m=\frac{n}{d}\cdot t$, $t\in Z$，则有

$$a^m=a^{\frac{n}{d}t}=\left(a^{\frac{n}{d}}\right)^t\in H.$$

由于 a^m 是 H_1 的生成元，所以 $H_1\subseteq H$. 又有 $|H_1|=|H|=d$，因而 $H_1=H$. ∎

例如 $G=\langle a\rangle$ 是无限循环群，任取 $a^i,a^j\in G$，若 $i\neq\pm j$，则 $\langle a^i\rangle$ 和 $\langle a^j\rangle$ 是 G 的不等的子群. 若不然必有 $a^i=a^{jt}$, $t\in Z$，即 a 是有限阶元，与 $G=\langle a\rangle$ 是无限阶循环群矛盾. 所以 G 有无限多个子群，即 $\langle e\rangle,\langle a\rangle,\langle a^2\rangle,\cdots$. 若 G 是 12 阶循环群 $\langle Z_{12},\oplus\rangle$，12 有六个正因子 1，

2,3,4,6,12.根据定理3.13,G有六个子群,分别由1,2,3,4,6和0来生成,正如图3.2的子群格所示.

【例3.16】 $G=\langle a\rangle$是n阶循环群,r是正整数.证明若a^r的阶是d,则$d=\frac{n}{(n,r)}$.

证 设$(n,r)=t$,由于$t|r$,故有

$$(a^r)^{\frac{n}{t}}=(a^n)^{\frac{r}{t}}=e^{\frac{r}{t}}=e.$$

根据定理3.8有$d\left|\frac{n}{t}\right.$.又由于$a^r$的阶是$d$,则

$$(a^r)^d=e.$$

从而有$n|rd$.这就推出$\frac{n}{t}\left|\frac{r}{t}\cdot d\right.$.因为$t=(n,r)$,即$\left(\frac{n}{t},\frac{r}{t}\right)=1$,所以有$\frac{n}{t}\left|d\right.$.

综合两方面的结果有$d=\frac{n}{t}=\frac{n}{(n,r)}$. ∎

【例3.17】 $G=\langle a\rangle$是n阶循环群,r,s是正整数,证明$\langle a^r\rangle=\langle a^s\rangle$当且仅当$(n,r)=(n,s)$.

证 根据定理3.13,对于n的每个正因子d,G中有且仅有一个d阶子群,所以

$$\langle a^r\rangle=\langle a^s\rangle\Leftrightarrow|\langle a^r\rangle|=|\langle a^s\rangle|.$$

而有限循环群的阶与它的生成元的阶相等,故有

$$|\langle a^r\rangle|=|\langle a^s\rangle|\Leftrightarrow|a^r|=|a^s|.$$

再根据例3.16知$|a^r|=\frac{n}{(n,r)}$,$|a^s|=\frac{n}{(n,s)}$,所以

$$|a^r|=|a^s|\Leftrightarrow\frac{n}{(n,r)}=\frac{n}{(n,s)}\Leftrightarrow(n,r)=(n,s).$$ ∎

§3.4 变换群和置换群

先定义变换和变换的乘法.

定义 3.9 设 A 是非空集合，$f: A \to A$ 称为 A 上的一个**变换**. 若 f 是双射的，则称 f 为 A 上的一个**一一变换**.

例如 $f: Z \to Z, f(x) = x$ 和 $g: Z \to Z, g(x) = -x$ 都是 Z 上的一一变换.

定义 3.10 设 f, g 是 A 上的两个变换，f 和 g 的合成① 称为 f 与 g 的**乘积**，简记作 fg.

不难证明 fg 也是 A 上的变换. 如果 f 和 g 都是 A 上的一一变换，则 fg 也是 A 上的一一变换.

定理 3.14 设 $E(A)$ 是 A 上的全体一一变换构成的集合，则 $E(A)$ 关于变换的乘法构成一个群.

证 任取 $f, g \in E(A)$，则 $fg \in E(A)$. 变换的乘法就是函数的合成，满足结合律. A 上的恒等变换 I_A 是一一变换，且是关于变换乘法的单位元. $\forall f \in E(A)$，f^{-1} 也是一一变换，且是 f 关于变换乘法的逆元. $E(A)$ 关于变换乘法构成群. ∎

我们称 $E(A)$ 为 A 的**一一变换群**，$E(A)$ 的子群称为 A 的**变换群**.

【例 3.18】 设 G 是群，$a \in G$. 定义 $f_a: G \to G, f_a(x) = ax$, $\forall x \in G$，则 f_a 是 G 上的变换，且是一一变换. 因为若 $f_a(x) = f_a(y)$, $x, y \in G$，则有 $ax = ay$. 由消去律可得 $x = y$，所以 f_a 是单射的. 此外对任意的 $y \in G$，有 $a^{-1}y \in G$，且 $f_a(a^{-1}y) = aa^{-1}y = y$. 这说明 f_a 又是满射的. 令

$$H = \{f_a \mid a \in G\}$$

是所有这种变换的集合，则 H 关于变换的乘法构成 G 上的变换群. 因为 $\forall f_a, f_b \in H$，$\forall x \in G$ 有

$$f_a f_b(x) = f_a(f_b(x)) = f_a(bx) = a(bx) = abx = f_{ab}(x),$$

即 $f_a f_b = f_{ab} \in H$. 结合律显然成立. f_e 是恒等变换，即 $\forall x \in G$,

① 关于合成的定义见《离散数学二分册：集合论与图论》

$f_e(x)=ex=x$，它是 H 中的单位元. 而 $\forall f_a\in H, f_{a^{-1}}$ 是 f_a 关于变换乘法的逆元，因为 $\forall x\in G$ 有

$$f_a f_{a^{-1}}(x)=f_a(f_{a^{-1}}(x))=aa^{-1}x=x.$$

所以 $f_a f_{a^{-1}}=f_e$，同理可证 $f_{a^{-1}}f_a=f_e$.

易见 $H\leqslant E(G)$.

当 A 是有穷集时，A 上的一一变换称为 A 上的**置换**. 当 $|A|=n$ 时称 A 上的置换为 **n 元置换**. 为了叙述上的方便，常将 A 记作 $\{1,2,\cdots,n\}$，这样就可以将 A 上的 n 元置换 σ 记作

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & & \sigma(n)\end{pmatrix}.$$

易见 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 恰为 $1,2,\cdots,n$ 的一个排列. 在 A 上的所有置换和 A 的所有排列之间存在着一一对应，n 元集有 $n!$ 个排列，所以有 $n!$ 个 n 元置换. 所有这些置换的集合记作 S_n. 根据定理 3.14，S_n 关于置换的乘法构成一个群，称为 **n 元对称群**，S_n 的子群称为 **n 元置换群**.

【例 3.19】 $S_3=\{\sigma_1,\sigma_2,\cdots,\sigma_6\}$. 其中

$$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\sigma_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \sigma_6=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

S_3 的运算表如表 3.2 所示.

表 3.2

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_4	σ_1	σ_2	σ_6	σ_5
σ_4	σ_4	σ_3	σ_6	σ_5	σ_1	σ_2
σ_5	σ_5	σ_6	σ_2	σ_1	σ_4	σ_3
σ_6	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

下面介绍 n 元置换的轮换表示与对换表示.

定义 3.11 设 $\sigma\in S_n$，若 σ 将 $\{1,2,\cdots,n\}$ 中的 k 个元素 $i_1,i_2,\cdots,i_k$ 进行如下变换：

$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \cdots,$

$\sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1,$

并且保持其它的元素不变，则可将 σ 记为 $(i_1 i_2 \cdots i_k)$，称为一个 **k 阶轮换**. 当 $k=1$ 时 $\sigma=(i_1)$，$i_1 \in \{1,2,\cdots,n\}$ 是恒等置换. 当 $k=2$ 时 $\sigma=(i_1 i_2)$ 称为一个**对换**.

例如(12)，(13)，(123) 都是 $\{1,2,3\}$ 上的轮换，其中(12)，(13) 是 2 阶轮换，也叫对换，(123) 是 3 阶轮换.

定义 3.12　设 $\sigma=(i_1 i_2 \cdots i_k)$ 和 $\tau=(j_1 j_2 \cdots j_s)$ 是两个轮换. 若 $\{i_1,i_2,\cdots,i_k\} \cap \{j_1,j_2,\cdots j_s\}=\varnothing$，则称 σ 和 τ 是**不相交的**.

例如 $\sigma,\tau \in S_5$，$\sigma=(134)$，$\tau=(25)$ 是不相交的.

定理 3.15　设 $\sigma,\tau \in S_n$，若 σ 与 τ 是不相交的，则 $\sigma\tau=\tau\sigma$.

证　令 $\sigma=(i_1 i_2 \cdots i_k)$，$\tau=(j_1 j_2 \cdots j_s)$. 将 $A=\{1,2,\cdots,n\}$ 划分成下面的三个子集：

$$A_1=\{i_1,i_2,\cdots,i_k\},$$
$$A_2=\{j_1,j_2,\cdots,j_s\},$$
$$A_3=A-(A_1 \cup A_2).$$

由于 σ 和 τ 是不相交的，$A_1 \cap A_2=\varnothing$.

任取 $l \in A$，若 $l \in A_3$，则 σ 和 τ 都不能使 l 改变，$\sigma\tau(l)=l=\tau\sigma(l)$.

若 $l \in A_1$，当 $l \neq i_k$ 时，有 $l=i_m$，$m \in \{1,2,\cdots,k-1\}$.

$$\sigma\tau(l)=\sigma\tau(i_m)=\sigma(\tau(i_m))=\sigma(i_m)=i_{m+1},$$
$$\tau\sigma(l)=\tau\sigma(i_m)=\tau(\sigma(i_m))=\tau(i_{m+1})=i_{m+1}.$$

当 $l=i_k$ 时有

$$\sigma\tau(l)=\sigma\tau(i_k)=\sigma(\tau(i_k))=\sigma(i_k)=i_1,$$
$$\tau\sigma(l)=\tau\sigma(i_k)=\tau(\sigma(i_k))=\tau(i_1)=i_1.$$

从而对任意 $l \in A_1$，有 $\sigma\tau(l)=\tau\sigma(l)$.

同理可证当 $l \in A_2$ 时也有 $\sigma\tau(l)=\tau\sigma(l)$.　∎

定理 3.16　任何 n 元置换都可以表成不相交的轮换之积，并且表法是唯一的. 这里的唯一性是指：若 σ 表成一系列不相交的轮换之积有两种表法

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t \text{ 和 } \sigma = \tau_1\tau_1\cdots\tau_l,$$

则有

$$\{\sigma_1,\sigma_2,\cdots,\sigma_t\} = \{\tau_1,\tau_1,\cdots,\tau_l\}.$$

证 设 $A = \{1,2,\cdots,n\}$，σ 是 A 上的 n 元置换. 在 σ 的作用下 A 中有 r 个元素发生了变化. 施归纳于 r.

$r = 0$，则 σ 是恒等置换 I_A，结论显然成立.

假设 $r < k$ 时结论成立，考虑 $r = k$ 的情况，即 σ 使 A 中的 k 个元素发生改变. 取 $i_1 \in A$ 且 $\sigma(i_1) \neq i_1$，令 $\sigma(i_1) = i_2$，然后取 $i_3 = \sigma(i_2)$，$i_4 = \sigma(i_3)$，$\cdots$，从而得到下面的序列

$$i_1, i_2 = \sigma(i_1),\ i_3 = \sigma(i_2),\cdots.$$

由于 $|A| = n$，必存在最小的正整数 m 使得 $i_1,i_2,\cdots,i_m$ 两两不等且 $i_{m+1} \in \{i_1,i_2,\cdots,i_m\}$. 若 $i_{m+1} = i_j$，$j \neq 1$，则有 $\sigma(i_{j-1}) = i_j = \sigma(i_m)$ 且 $i_{j-1} \neq i_m$. 这与 σ 的单射性矛盾，所以必有 $i_{m+1} = i_1$. 令 $\tau_1 = (i_1i_2\cdots i_m)$，$\tau_1$ 是由 σ 中分解出来的第一个轮换，$\sigma = \tau_1\sigma'$. 由 σ 的单射性知 σ' 与 τ_1 是不相交的，σ' 仅变动 A 中剩下的 $k - m$ 个元素. 由归纳假设 σ' 也可以表成一系列不交的轮换之积，即

$$\sigma' = \tau_2\tau_3\cdots\tau_l,$$

其中 $\tau_2,\tau_3,\cdots,\tau_l$ 两两不交. 从而得到 σ 的不相交轮换表示 $\sigma = \tau_1\tau_2\tau_3\cdots\tau_l$.

下面证明表法的唯一性. 设

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t \text{ 和 } \sigma = \tau_1\tau_2\cdots\tau_l$$

都是 σ 的不相交轮换表示. 令 $X = \{\sigma_1,\sigma_2,\cdots,\sigma_t\}$，$Y = \{\tau_1,\tau_2,\cdots,\tau_l\}$，我们只需证明 $X = Y$.

任取 $\sigma_j \in X$，不妨设 $\sigma_j = (i_1i_2\cdots i_m)$，$m > 1$. 由于 $\tau_1\tau_2\cdots\tau_l$ 也是 σ 的不相交轮换表示，$\sigma(i_1) \neq i_1$，所以必存在某个 $\tau_s \in Y$ 使得 i_1 在 τ_s 中出现. 对于 $k = 1,2,\cdots,m-1$，若 i_k 在 τ_s 中出现，则 $i_{k+1} = \sigma(i_k)$ 也在 τ_s 中出现，否则与 τ_s 是轮换且与 $\tau_1,\cdots,\tau_{s-1},\tau_{s+1},\cdots,\tau_l$ 不相交矛盾. 这

就证明了 $i_1, i_2, \cdots, i_m$ 必依次出现于 τ_s 中. 另一方面,若 τ_s 中除了 $i_1, i_2, \cdots, i_m$ 以外还含有其它元素 u,则 u 只能在 i_m 之后出现,即 $\tau_s(i_m) = u$,从而得到 $\sigma(i_m) = \tau_s(i_m) = u$ 和 $\sigma(i_m) = \sigma_j(i_m) = i_1$,与 σ 是映射矛盾. 因此 $\tau_s = \sigma_j$,即 $\sigma_j \in Y$. 由于 σ_j 的任意性,$X \subseteq Y$.

同理可证 $Y \subseteq X$,从而有 $X = Y$. ∎

【例 3.20】 设 $\sigma, \tau \in S_8$,且

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 8 & 1 & 4 & 6 & 7 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 8 & 7 & 6 & 1 & 4 \end{pmatrix},$$

写出 σ 和 τ 的不相交轮换表示.

解 先从 σ 中取出 1,$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 5, \sigma(5) = 1$,这就得到第一个轮换(1235). 然后从剩下的元素中取出 4,$\sigma(4) = 8, \sigma(8) = 7, \sigma(7) = 6, \sigma(6) = 4$,从而得到第二个轮换(4876). 不存在剩下的元素了,$\sigma = (1235)(4876)$.

类似的分析可得 $\tau = (157)(2)(3)(48)(6)$. 在 τ 的表示中可以省略所有的 1 阶轮换,如(2),(3) 和(6),最后得到 $\tau = (157)(48)$.

注意当 σ 是恒等置换时,不可以省去 σ 中所有的 1 阶轮换,应该保留一个$(i), i \in \{1, 2, \cdots, n\}$.

定义 3.13 设 $\sigma \in S_n$ 已经用不交的轮换之积表出,对于 $k = 1, 2, \cdots, n$,令 $c_k(\sigma)$ 表示 σ 中的 k 阶轮换的个数,则 $1^{c_1(\sigma)} 2^{c_2(\sigma)} \cdots n^{c_n(\sigma)}$ 称为 σ 的**轮换指数**. 若某个 $c_k(\sigma) = 0, k \in \{1, 2, \cdots, n\}$,可在轮换指数的表示式里省去对应的 $c_k(\sigma)$ 项.

例如 $S_3 = \{(1), (12), (13), (23), (123), (132)\}$,则(1)的轮换指数为 1^3. 因为(1) = (1)(2)(3),是 3 个 1 阶轮换之积. 在轮换指数的表示式中应该算上所有省略的 1 阶轮换. (12),(13),(23) 的轮换指数为 $1^1 2^1$. (123) 和(132) 的轮换指数为 3^1. 再考虑例 3.20 中的两个 8 元置换 σ 和 τ,σ 的轮换指数为 4^2,τ 的轮换指数为 $1^3 2^1 3^1$.

由于置换的表示式中任意两个轮换都是不交的，每个轮换的元素都不相同. $1,2,\cdots,n$ 这 n 个元素分配到所有的轮换之中，所有轮换（包括 1 阶轮换）的元素总数必等于 n，即

$$1\cdot c_1(\sigma)+2\cdot c_2(\sigma)+\cdots+n\cdot c_n(\sigma)=n.$$

例如 8 元置换 τ 的轮换指数为 $1^3 2^1 3^1$，满足

$$1\cdot 3+2\cdot 1+3\cdot 1=8.$$

下面考虑 n 元置换的对换表示. 根据前面的分析可以知道，任何 n 元置换都可以表为不交的轮换之积. 如果任何轮换都可以表成对换之积，那么 n 元置换就可以表成对换之积.

定理 3.17　设 $\sigma=(i_1i_2\cdots i_k)$ 是 $A=\{1,2,\cdots,n\}$ 上的 k 阶轮换，$k>1$，则 $\sigma=(i_1i_k)(i_1i_{k-1})\cdots(i_1i_2)$.

证　对 k 进行归纳，当 $k=2$ 时命题显然为真. 假设 $k=t$ 时结论为真，考虑 $\sigma=(i_1i_2\cdots i_{t+1})$ 的情况. 令 $\sigma_1=(i_1i_{t+1})$，$\sigma_2=(i_1i_2\cdots i_t)$，下面证明 $\sigma=\sigma_1\sigma_2$.

任取 $l\in A$. 若 $l\in\{i_1,i_2,\cdots,i_{t-1}\}$，不妨设 $l=i_m$，则

$$\sigma(l)=\sigma(i_m)=i_{m+1},$$

$$\sigma_1\sigma_2(l)=\sigma_1(\sigma_2(l))=\sigma_1(i_{m+1})=i_{m+1};$$

若 $l=i_t$，则

$$\sigma(l)=i_{t+1}=\sigma_1(i_1)=\sigma_1(\sigma_2(i_t))=\sigma_1\sigma_2(i_t)=\sigma_1\sigma_2(l);$$

若 $l=i_{t+1}$，则

$$\begin{aligned}\sigma(l)&=\sigma(i_{t+1})=i_1=\sigma_1(i_{t+1})=\sigma_1(\sigma_2(i_{t+1}))\\&=\sigma_1\sigma_2(i_{t+1})=\sigma_1\sigma_2(l);\end{aligned}$$

若 $l\notin\{i_1,i_2,\cdots,i_{t+1}\}$，则

$$\sigma(l)=l=\sigma_1(l)=\sigma_1(\sigma_2(l))=\sigma_1\sigma_2(l).$$

综上所述，$\forall l\in A$ 都有 $\sigma(l)=\sigma_1\sigma_2(l)$，即

$$\sigma=\sigma_1\sigma_2=(i_1i_{t+1})\sigma_2.$$

由归纳假设，$\sigma_2=(i_1i_2\cdots i_t)$ 可以表为

$$(i_1i_t)(i_1i_{t-1})\cdots(i_1i_2),$$

所以

$$\sigma = (i_1 i_{t+1})(i_1 i_t)\cdots(i_1 i_2).$$

根据数学归纳法命题得证. ∎

【例 3.21】 考虑例 3.20 中的 σ 和 τ,它们的对换表示分别为:

$$\sigma = (15)(13)(12)(46)(47)(48),$$

$$\tau = (17)(15)(48).$$

定理 3.16 告诉我们,当把一个 n 元置换表成不相交轮换之积时,表法是唯一的. 但在表成对换之积时,对换是允许相交的,并且表法也不是唯一的. 例如,例 3.21 中的 τ 也可以表为(17) (57) (15) (17) (48). 尽管表法不唯一,但可以证明不同表示中的对换个数的奇偶性是不变的. 为了完成这个证明先给出一些有关排列的知识.

定义 3.14 设 $i_1 i_2 \cdots i_n$ 是 $1,2,\cdots,n$ 的一个排列. 若 $i_k > i_l$ 且 $k < l$,则称 $i_k i_l$ 是一个**逆序**. 排列中逆序的总数称为这个排列的**逆序数**.

例如排列 25431 中有 7 个逆序: 21,51,41,31,53,43,54. 25431 的逆序数是 7.

定理 3.18 $\sigma \in S_n$,且 $\sigma(j) = i_j, j = 1,2,\cdots,n$,则在 σ 的对换表示中对换个数的奇偶性与排列 $\pi = i_1 i_2 \cdots i_n$ 的逆序数的奇偶性相一致.

证 令 $\alpha(\sigma)$ 是 σ 的对换表示中对换的个数,$\lambda(\pi)$ 是排列 π 的逆序数. 对 n 进行归纳.

$n = 1$,则 $\sigma = (1)$, $\alpha(\sigma) = 0$. 而 1 阶排列的逆序数也为 0. 命题为真.

假设 $n = k$ 时结论为真,考虑 $k + 1$ 元置换 σ. 若 $\sigma(k + 1) = k + 1$,则 $\sigma \upharpoonright \{1,2,\cdots,k\}$ 是 k 元置换,且所对应的排列为 $i_1 i_2 \cdots i_k$. 易见

$$\alpha(\sigma) = \alpha(\sigma \upharpoonright \{1,2,\cdots,k\}).$$

$$\lambda(i_1 i_2 \cdots i_k (k + 1)) = \lambda(i_1 i_2 \cdots i_k).$$

由归纳假设,$\alpha(\sigma \upharpoonright \{1,2,\cdots,k\})$ 与 $\lambda(i_1 i_2 \cdots i_k)$ 的奇偶性一致,所以 $\alpha(\sigma)$ 与 $\lambda(i_1 i_2 \cdots i_k (k + 1))$ 奇偶性也是一致的.

若 $\sigma(k+1)=s$，$s\neq k+1$. 必存在 $l\in\{1,2,\cdots,k\}$ 使得 $\sigma(l)=k+1$. 令 σ 对应的排列为 π，则 $\pi=i_1i_2\cdots i_{l-1}(k+1)i_{l+1}\cdots i_ks$. 如下构造 σ'，使得 $\sigma'=(k+1,s)\sigma$，则 σ' 所对应的排列为 $\pi'=i_1i_2\cdots i_{l-1}si_{l+1}\cdots i_k(k+1)$. 易见 $\alpha(\sigma)$ 与 $\alpha(\sigma')$ 的奇偶性相反，$\lambda(\pi)$ 与 $\lambda(\pi')$ 的奇偶性也相反. 由 $\sigma'(k+1)=k+1$，根据前面的分析，$\alpha(\sigma')$ 与 $\lambda(\pi')$ 的奇偶性一致. 所以 $\alpha(\sigma)$ 与 $\lambda(\pi)$ 的奇偶性也一致. ∎

由以上定理可知当把 n 元置换表成对换之积时，表示式中对换个数的奇偶性是不变的. 根据这个性质可以将 n 元置换分为奇置换和偶置换.

定义 3.15 如果 n 元置换 σ 可表成奇数个对换的连乘积，则称 σ 为**奇置换**，否则称为**偶置换**.

【例 3.22】 设 A_n 是 S_n 中全体偶置换的集合，则 A_n 是 S_n 的子群，称为 **n 元交代群**(或**交错群**).

证 因为 A_n 是有穷集，我们只须证明 A_n 对 S_n 中的乘法封闭即可. 任取 $\sigma,\tau\in A_n$，σ,τ 都可表成偶数个对换之积，则 $\sigma\tau$ 也可表成偶数个对换之积，即 $\sigma\tau\in A_n$，$A_n\leqslant S_n$. ∎

不难验证 $|A_n|=\frac{1}{2}n!$. 例如 $S_3=\{(1),(12),(13),(23),(123),(132)\}$，其中 (1)，(123) 和 (132) 是偶置换，即 $A_3=\{(1),(123),(132)\}$.

下面考虑置换群中元素的阶.

定理 3.19 G 是 n 元置换群.

(1) $\sigma\in G$，$\sigma=(i_1i_2\cdots i_k)$，则 $|\sigma|=k$.

(2) $\tau\in G$，$\tau=\tau_1\tau_2\cdots\tau_l$ 是不相交轮换的分解式. 若 τ_i 是 k_i 阶轮换，$i=1,2,\cdots,l$，则 τ 的阶是 $k_1,k_2,\cdots,k_l$ 的最小公倍数，即 $|\tau|=[k_1,k_2,\cdots,k_l]$.

证 (1) $\sigma^k=(i_1i_2\cdots i_k)^k=(i_1)$，假若 $j<k$，则 $\sigma^j(i_1)=(i_1i_2\cdots i_k)^j(i_1)=i_{j+1}\neq i_1$. 这就证明了 $|\sigma|=k$.

(2) 设 $|\tau| = t$, $[k_1,k_2,\cdots,k_l] = d$. 由于 $\tau_1,\cdots,\tau_l$ 是不交的，则

$$\tau^d = \tau_1^d\tau_2^d\cdots\tau_l^d = (1),$$

因此有 $t|d$.

另一方面，$\tau^t = (1)$，由于 $\tau_1,\tau_2,\cdots,\tau_l$ 两两不相交必有 $\tau_i^t = (1)$，$i = 1,2,\cdots,l$. 根据(1) 部分的证明知 $|\tau_i| = k_i$，因此对于所有的 $i \in \{1,2,\cdots,l\}$ 有 $k_i|t$，t 是 $k_1,k_2,\cdots,k_l$ 的公倍数. 由于 d 是 $k_1,k_2,\cdots,k_l$ 的最小公倍数，必有 $d|t$.

综合上面的结论有 $t = d$，即 $|\tau| = [k_1,k_2,\cdots,k_l]$. ∎

下面是一个置换群的例子.

【例 3.23】 图 3.3 是一个 2×2 的方格图形. 它可以围绕中心旋转，也可以围绕对称轴翻转，但要求经过这样的变动以后的图形要与原来的图形重合(方格中的数字可以改变). 例如，当它绕中心逆时针旋转 90° 以后，原来的数字 1,2,3 和 4 分别变成了 2,3,4 和 1. 可以把这个变化看作是{1,2,3,4}上的一个置换(1234). 下面给出所有可能的置换：

1	2
4	3

图 3.3

$\sigma_1 = (1)$ 绕中心逆时针转 0°；

$\sigma_2 = (1234)$ 绕中心逆时针转 90°；

$\sigma_3 = (13)(24)$ 绕中心逆时针转 180°；

$\sigma_4 = (1432)$ 绕中心逆时针转 270°；

$\sigma_5 = (12)(34)$ 绕垂直轴翻转 180°；

$\sigma_6 = (14)(23)$ 绕水平轴翻转 180°；

$\sigma_7 = (24)$ 绕西北 — 东南轴翻转 180°；

$\sigma_8 = (13)$ 绕西南 — 东北轴翻转 180°.

表 3.3 给出了它们的运算表. 令 $D_4 = \{\sigma_1,\sigma_2,\cdots,\sigma_8\}$，易见 D_4 关于置换的乘法是封闭的. $\sigma_1 = (1)$ 是单位元. 且 $\sigma_1^{-1} = \sigma_1$, $\sigma_2^{-1} = \sigma_4$, $\sigma_3^{-1} = \sigma_3$, $\sigma_4^{-1} = \sigma_2$, $\sigma_5^{-1} = \sigma_5$, $\sigma_6^{-1} = \sigma_6$, $\sigma_7^{-1} = \sigma_7$, $\sigma_8^{-1} = \sigma_8$. D_4 构成一个群，且是 S_4 的子群.

表 3.3

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_2	σ_2	σ_3	σ_4	σ_1	σ_8	σ_7	σ_5	σ_6
σ_3	σ_3	σ_4	σ_1	σ_2	σ_6	σ_5	σ_8	σ_7
σ_4	σ_4	σ_1	σ_2	σ_3	σ_7	σ_8	σ_6	σ_5
σ_5	σ_5	σ_7	σ_6	σ_8	σ_1	σ_3	σ_2	σ_4
σ_6	σ_6	σ_8	σ_5	σ_7	σ_3	σ_1	σ_4	σ_2
σ_7	σ_7	σ_6	σ_8	σ_5	σ_4	σ_2	σ_1	σ_3
σ_8	σ_8	σ_5	σ_7	σ_6	σ_2	σ_4	σ_3	σ_1

§3.5 群的分解

群通常可以按两种方法分解：陪集分解或共轭类分解. 由陪集分解可以得到 Lagrange 定理，按共轭类分解可以得到群的分类方程.

定义 3.16 G 是群，H 是 G 的子群，$a \in G$. 令

$$Ha = \{ha \mid h \in H\},$$

称 Ha 是子群 H 在 G 中的一个**右陪集**.

【例 3.24】 $G = S_3$, $H = A_3$，则

$$H(23) = \{(23),(12),(13)\} = H(12) = H(13),$$

$$H(1) = \{(1),(123),(132)\} = H(123) = H(132).$$

下面给出右陪集的性质.

定理 3.20 设 G 是群，H 是 G 的子群，则

(1) $He = H$;

(2) $\forall a \in G$, $a \in Ha$.

证 (1) $He = \{he \mid h \in H\} = \{h \mid h \in H\} = H$;

(2) $\forall a \in G, a = ea \in Ha$. ∎

定理 3.21 设 G 是群，H 是 G 的子群，则 $\forall a \in G, Ha \approx H$.

证 令 $\varphi: H \to Ha$, $\varphi(h) = ha$, $\forall h \in H$，则 φ 是 H 到 Ha 的函数. 任取 $ha \in Ha$，必有 $h \in H$，且 $\varphi(h) = ha$，φ 是满射的. 若 $\varphi(h_1) = \varphi(h_2)$，即 $h_1a = h_2a$，由 G 中消去律可知 $h_1 = h_2$，这就证明了 φ 的

单射性. 由等势定义有 $H \approx Ha$，即 $Ha \approx H$. ∎

定理 3.22　G 是群，H 是 G 的子群，$\forall a,b \in G$ 有

$$a \in Hb \Leftrightarrow Ha = Hb \Leftrightarrow ab^{-1} \in H.$$

证　先证 $a \in Hb \Rightarrow Ha = Hb$. 由 $a \in Hb$，必存在 $h_1 \in H$ 使得 $a = h_1 b$. 那么 $b = h_1^{-1}a$. 任取 $ha \in Ha$，则 $ha = hh_1 b$. 由于 $H \leqslant G$，$hh_1 \in H$，则有 $ha \in Hb$，这就推出 $Ha \subseteq Hb$. 任取 $hb \in Hb$，由 $b = h_1^{-1}a$ 得 $hb = hh_1^{-1}a$. 而 $hh_1^{-1} \in H$，所以 $hb \in Ha$，这就证出 $Hb \subseteq Ha$. 综合以上结果有 $Ha = Hb$.

反之，若 $Ha = Hb$，根据定理 3.20，$\forall a \in G$ 有 $a \in Ha$，从而有 $a \in Hb$.

再证　$Ha = Hb \Leftrightarrow ab^{-1} \in H$.

$$Ha = Hb \Leftrightarrow a \in Hb \Leftrightarrow \exists\, h(h \in H \wedge a = hb)$$
$$\Leftrightarrow \exists\, h(h \in H \wedge ab^{-1} = h) \Leftrightarrow ab^{-1} \in H.$$ ∎

定理 3.23　G 是群，H 是 G 的子群，在 G 上定义二元关系 R，$\forall a,b \in G$ 有

$$aRb \Leftrightarrow ab^{-1} \in H,$$

则 R 为 G 上的等价关系，且 $[a]_R = Ha$.

证　$\forall a \in G$，$aa^{-1} = e \in H$，即 aRa 成立，R 在 G 上是自反的.

$\forall a,b \in G$ 有

$$aRb \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow bRa.$$

这就推出 R 在 G 上是对称的.

$\forall a,b,c \in G$ 有

$$aRb \wedge bRc \Rightarrow ab^{-1} \in H \wedge bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} \in H$$
$$\Rightarrow ac^{-1} \in H \Rightarrow aRc.$$

所以 R 在 G 上是传递的. R 是 G 上的等价关系.

$\forall b \in G$ 有

$$b \in [a]_R \Leftrightarrow aRb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb \Leftrightarrow b \in Ha.$$

这就推出 $[a]_R = Ha$. ∎

定理 3.24　G 是群，H 是 G 的子群，则 $\forall a,b \in G, Ha \cap Hb = \varnothing$ 或 $Ha = Hb$，且 $\bigcup_{a\in G} Ha = G$.

证　根据集合论中有关等价类的定理可直接得到.

【例 3.25】　$G = S_3$，$H = \{(1),(12)\}$，则 H 的所有右陪集是：

$H(1) = H(12) = H$，

$H(13) = \{(13), (132)\} = H(132)$，

$H(23) = \{(23), (123)\} = H(123)$.

每个右陪集都是等势的，不同的右陪集是不交的，所有右陪集的并就等于 S_3.

【例 3.26】　$G = \langle R^*, \cdot \rangle$，其中 $R^* = R - \{0\}$ 是非零实数的集合，$\cdot$ 是普通乘法. $H = \{1, -1\}$ 是 G 的子群，$\forall r \in R^*$，$Hr = \{r, -r\}$，且有 $\bigcup_{r\in R^*} Hr = R^*$.

以上讨论了子群 H 的右陪集，类似地可以定义 H 的左陪集. $\forall a \in G$，令

$$aH = \{ah \mid h \in H\},$$

则 aH 是 H 在 G 中的一个**左陪集**. 例如 $G = S_3$，$H = \{(1),(12)\}$，则 H 在 G 中的全体左陪集是：

$(1)H = H$，$(12)H = H$，

$(13)H = \{(13),(123)\}$，$(123)H = \{(123),(13)\}$，

$(23)H = \{(23),(132)\}$，$(132)H = \{(132),(23)\}$.

和例 3.25 相比，只有 $(1)H = H(1)$，$(12)H = H(12)$，而对于 S_3 中的其它置换 σ，$\sigma H \neq H\sigma$.

和右陪集的性质类似，也可以得到左陪集的性质.

定理 3.25　设 G 是群，H 是 G 的子群，则

(1) $eH = H$；

(2) $\forall a \in G$，$a \in aH$；

(3) $\forall a \in G$，$aH \approx H$；

(4) $\forall a,b \in G$, $a \in bH \Leftrightarrow aH = bH \Leftrightarrow a^{-1}b \in H$;

(5) 在 G 上定义二元关系 R, $\forall a,b \in G, aRb \Leftrightarrow a^{-1}b \in H$,则 R 为 G 上的等价关系,且 $[a]_R = aH$;

(6) $\forall a,b \in G, aH \cap bH = \varnothing$ 或 $aH = bH$,且 $\bigcup_{a\in G} aH = G$.

证明留作练习.

下面介绍 Lagrange 定理,先给出一个引理.

引理 G 是群,H 是 G 的子群,则 H 在 G 中的左陪集数与右陪集数相等.

证 令 S,T 分别为 G 的右和左陪集的集合.

定义 φ: $S \to T$, $\varphi(Ha) = a^{-1}H, \forall Ha \in S$.

我们必须验证 φ 是良定义的,也就是说如果 $Ha = Hb$ 则有 $\varphi(Ha) = \varphi(Hb)$. 根据右陪集和左陪集的性质有

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H$$
$$\Leftrightarrow a^{-1}H = b^{-1}H \Leftrightarrow \varphi(Ha) = \varphi(Hb),$$

这就证明 φ 是良定义的,并且是单射的. 然后我们证明 φ 是满射的. 任取 $xH \in T$,则 $x \in G$. 因为 G 是群,$x^{-1} \in G, Hx^{-1} \in S$ 且 $\varphi(Hx^{-1}) = (x^{-1})^{-1}H = xH$. 根据等势定义有 $S \approx T$. ▮

定义 3.17 G 是群,H 是 G 的子群. H 在 G 中的右陪集数(或左陪集数)叫做 **H 在 G 中的指数**,记作 $[G:H]$, 若 $H = \{e\}$,也可以将 $[G:H]$ 记作 $[G:1]$.

定理 3.26 (Lagrange 定理) 设 G 是有限群, H 是 G 的子群, 则

$$|G| = [G:H]\ |H|.$$

证 设 $[G:H] = r$,根据定理 3.24 有

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r,$$

其中 $a_1,a_2,\cdots,a_r$ 分别为 H 的 r 个陪集的代表元素. 由于 $Ha_1,Ha_2,\cdots,Ha_r$ 两两不相交,所以 G 的元素数等于这些陪集的元素数之和,即

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_r|.$$

再根据定理 3.21，所有的陪集都和 H 等势，即 $\forall a \in G, Ha \approx H$，故 $|Ha| = |H|$，代入上式得

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{r\text{个}} = r|H| = [G:H]\,|H|. \quad \blacksquare$$

Lagrange 定理告诉我们：若 G 是有限群，则 G 的子群的阶是 G 的阶的因子. 但它的逆命题不一定为真. 换句话说，如果正整数 d 是有限群 G 的阶的因子，但 G 中不一定存在 d 阶子群. 例如 $G = A_4$，则 $|G| = 12$，6 是 $|G|$ 的因子，但 A_4 没有 6 阶子群.

推论 1 G 是 n 阶群，则 G 中每个元素的阶是 n 的因子，且 $\forall a \in G$ 有 $a^n = e$.

证 $\forall a \in G$，令 $H = \langle a \rangle$，则 H 是 G 的子群. 根据 Lagrange 定理，$|H|$ 是 n 的因子. 又由于 H 是循环群，$|H|$ 就是生成元 a 的阶，所以 a 的阶是 n 的因子. 可以将 n 表为 $|a|t$，t 是整数. 从而有

$$a^n = a^{|a|t} = (a^{|a|})^t = e^t = e. \quad \blacksquare$$

推论 2 阶为素数的群是循环群.

证 设群 G 的阶为 p，p 是素数. 由 $p \geqslant 2$，G 中必存在 $a \in G$，$a \neq e$. 令 $H = \langle a \rangle$，则 H 是 G 的子群. 根据 Lagrange 定理 $|H| = 1$ 或 $|H| = p$.

若 $|H| = 1$，则 $|a| = |H| = 1$，与 $a \neq e$ 矛盾，所以 $|H| = p$. 又由于 $|G| = p$，必有 $H = G$，G 是循环群. $\blacksquare$

利用 Lagrange 定理和两个推论可以分析有限群的结构.

【例 3.27】 证明 6 阶群一定含有 3 阶元.

证 设 G 是 6 阶群. 根据推论 1，G 中元素的阶是 6 的因子，所以 G 中只可能存在 1 阶、2 阶、3 阶和 6 阶元.

若 G 中含有 6 阶元，比如说是 a，则 a^2 就是 G 中的 3 阶元.

若 G 中不含有 6 阶元，则 G 中的非单位元只可能为 2 阶或 3 阶元. 下面用反证法证明 G 中必含 3 阶元. 若不然，G 中所有元素 a 都满

足 $a^2=e$，即 $a=a^{-1}$. 任取 $a,b\in G$，则有

$$ab=(ab)^{-1}=b^{-1}a^{-1}=ba.$$

G 是 Abel 群. 取 G 中非单位元 a 和 b，令 $H=\{e,a,b,ab\}$，易证 H 是 G 的子群. 但 $|H|\nmid|G|$，与 Lagrange 定理矛盾. ∎

【例 3.28】 证明每个阶小于 6 的群都是 Abel 群.

证 由推论 2 可知 2 阶、3 阶和 5 阶群是循环群，也是 Abel 群. 1 阶群是平凡群，也是 Abel 群. 下面考虑 4 阶群. 设 G 是 4 阶群，根据推论 1，G 中只可能有 1 阶、2 阶和 4 阶元.

若 G 中含有 4 阶元，比如说是 a，则 G 是循环群 $\langle a\rangle$，显然是 Abel 群.

若 G 中只含有 1 阶和 2 阶元，根据例 3.27 的证明 G 也是 Abel 群，从同构的意义上说就是 Klein 四元群. ∎

【例 3.29】 证明 6 阶群若不是循环群就同构于 S_3.

证 设 G 是 6 阶群. 由推论 1，G 中只可能含有 1 阶、2 阶、3 阶和 6 阶元.

若 G 中含 6 阶元，比如说是 a，则 $G=\langle a\rangle$ 是循环群.

若 G 中不含 6 阶元，由例 3.27 知 G 中必含 3 阶元. 令这个 3 阶元是 a. 取 $c\in G, c\neq e, c\neq a, c\neq a^2$，则 $ac\neq e$，否则有 $c=a^{-1}=a^2$，与 c 的选取矛盾. $ac\neq a$，否则由消去律有 $c=e$. 类似地可以证明 e, a,a^2,c,ac,a^2c 是两两不同的元素. 令

$$G=\{e,a,a^2,c,ac,a^2c\}.$$

先考虑 c^2. 显然 $c^2\neq c,ac,a^2c$. 若 $c^2=a^2$，因 a 是 3 阶元知 $a^2\neq e$，所以 $c^2\neq e$. c 只能是 3 阶元，从而推出

$$a^2c=c^2c=c^3=e,$$

与 $a^2c\neq e$ 矛盾. 若 $c^2=a$，由 a 是 3 阶元知 $c^2\neq e$. c 只能是 3 阶元，这就推出

$$ac=c^2c=c^3=e,$$

与 $ac\neq e$ 矛盾. 综合以上结果必有 $c^2=e$，c 是 2 阶元.

再考虑 ca，显然 $ca \neq e, a, a^2$ 和 c. 若 $ca = ac$，a 和 c 是可交换的且它们的阶互素，由例 3.6 可知 ca 的阶是 6，与 G 中不含 6 阶元矛盾. 由此可知 $ca = a^2c$. 从而有

$$(ca)^2 = caca = caa^2c = e,$$

所以 $a^2c = ca$ 是 2 阶元.

最后考虑 ac，由

$$(ac)^2 = acac = a(a^2c)c = e$$

可知 ac 也是 2 阶元.

通过以上的分析可以得到 G 的运算表. 请看表 3.4.

令 $f: G \to S_3$，f: $e \mapsto (1)$，$a \mapsto (123)$，$a^2 \mapsto (132)$，$c \mapsto (12)$，$ac \mapsto (13)$，$a^2c \mapsto (23)$，将表 3.4 中 G 的元素 x 用 $f(x)$ 代替就得到表 3.5，恰好就是 S_3 的运算表. 这就验证了 $\forall x, y \in G$ 有

$$f(xy) = f(x)f(y),$$

表 3.4

	e	c	ac	a^2c	a	a^2
e	e	c	ac	a^2c	a	a^2
c	c	e	a^2	a	a^2c	ac
ac	ac	a	e	a^2	c	a^2c
a^2c	a^2c	a^2	a	e	ac	c
a	a	ac	a^2c	c	a^2	e
a^2	a^2	a^2c	c	ac	e	a

表 3.5

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

f 是 G 到 S_3 的同态. 又知 f 是双射,所以 f 是 G 到 S_3 的同构. ∎

以上讨论的是群的陪集分解,现在考虑群的共轭类分解.

定义 3.18　设 G 是群,在 G 上定义二元关系 R,$\forall a,b \in G$ 有

$$aRb \Leftrightarrow \exists\, x(x \in G \wedge a = xbx^{-1}),$$

则称 R 是 G 上的**共轭关系**. 如果 aRb,则称 b 是 a 的**共轭**.

定理 3.27　群 G 上的共轭关系是 G 上的等价关系.

证　$\forall a \in G$ 有 $a = eae^{-1}$,即 aRa,R 在 G 上是自反的.

$\forall a,b \in G$ 有

$$aRb \Rightarrow \exists\, x(x \in G \wedge a = xbx^{-1}) \Rightarrow \exists\, x(x \in G \wedge b = x^{-1}ax)$$
$$\Rightarrow \exists\, x^{-1}(x^{-1} \in G \wedge b = x^{-1}a(x^{-1})^{-1}) \Rightarrow bRa,$$

R 在 G 上是对称的.

$\forall a,b,c \in G$ 有

$$aRb \wedge bRc$$
$$\Rightarrow \exists\, x(x \in G \wedge a = xbx^{-1}) \wedge \exists\, y(y \in G \wedge b = ycy^{-1})$$
$$\Rightarrow \exists\, x\, \exists\, y(x,y \in G \wedge a = x(ycy^{-1})x^{-1})$$
$$\Rightarrow \exists\, x\, \exists\, y(xy \in G \wedge a = xyc(xy)^{-1}) \Rightarrow aRc.$$

R 在 G 上是传递的.

综合以上结果,R 是 G 上的等价关系. ∎

定义 3.19　R 是群 G 上的共轭关系,$a \in G$,a 的等价类 $[a]_R$ 称作 a 的**共轭类**,简记作 $\overline{a}$.

【例 3.30】　$G = S_3$,G 中的全体共轭类是:

$\overline{(1)} = \{(1)\}$.

$\overline{(12)} = \{(12),(13),(23)\} = \overline{(13)} = \overline{(23)}$.

$\overline{(123)} = \{(123),(132)\} = \overline{(132)}$.

易见 S_3 中同一共轭类的元素都具有相同的轮换指数,可以证明这个性质对 S_n 也是成立的. 证明留作练习.

定理 3.28　G 是群,C 是 G 的中心,则 $\forall a \in G$ 有

$$a \in C \Leftrightarrow \overline{a} = \{a\}.$$

证　必要性. 设 $a \in C$，则对任意的 y，

$y \in \overline{a} \Leftrightarrow \exists\, x(x \in G \wedge y = xax^{-1}) \Leftrightarrow \exists\, x(x \in G \wedge yx = xa)$
$\exists\, x(x \in G \wedge yx = ax) \Leftrightarrow y = a \Leftrightarrow y \in \{a\}$.

充分性.　任取 $x \in G$，则 $xax^{-1} \in \overline{a} = \{a\}$，即 $xax^{-1} = a$. 因此有 $xa = ax$，$a \in C$. ∎

由于共轭关系是群 G 上的等价关系，可以把群 G 按共轭类分解. 下面考虑共轭类的计数.

定义 3.20　G 是群，$a \in G$，令

$$N(a) = \{x \mid x \in G \wedge xa = ax\},$$

称 $N(a)$ 是 a 的**正规化子**.

【例 3.31】　$G = S_3$，则 G 中所有元素的正规化子是：

$N((1)) = G$，

$N((12)) = \{(1),\ (12)\}$，

$N((13)) = \{(1),\ (13)\}$，

$N((23)) = \{(1),\ (23)\}$，

$N((123)) = N((132)) = \{(1),\ (123), (132)\}$.

关于正规化子有以下的定理.

定理 3.29　G 是群，则 $\forall a \in G$，$N(a)$ 是 G 的子群.

证明留作练习.

定理 3.30　G 是有限群，则 $\forall a \in G$ 有

$$|\overline{a}| = [G : N(a)].$$

证　任取 $x, y \in G$ 有

$$xax^{-1} = yay^{-1} \Leftrightarrow ax^{-1}y = x^{-1}ya$$
$$\Leftrightarrow x^{-1}y \in N(a) \Leftrightarrow xN(a) = yN(a).$$

这说明 x 和 y 确定 a 的同一共轭当且仅当 x 和 y 确定 $N(a)$ 的同一左陪集. 因此与 a 共轭的元素数就等于 $N(a)$ 在 G 中的左陪集数，即 $|\overline{a}| = [G : N(a)]$. ∎

定理 3.31　（群的分类方程）G 是有限群，C 是 G 的中心. 设 G 中

至少含有两个元素的共轭类有 k 个，且 $a_1,a_2,\cdots,a_k$ 分别为这 k 个共轭类的代表元素，则

$$|G| = |C| + [G:N(a_1)] + [G:N(a_2)] + \cdots + [G:N(a_k)].$$

证 设 C 中含有 l 个元素，记作 $a_{k+1},a_{k+2},\cdots,a_{k+l}$. 由定理3.28，对于 $i=1,2,\cdots,l$ 有 $\overline{a}_{k+i}=\{a_{k+i}\}$. 根据共轭类的性质有

$$G=\overline{a}_1\cup\overline{a}_2\cup\cdots\cup\overline{a}_k\cup\overline{a}_{k+1}\cup\cdots\cup\overline{a}_{k+l}.$$

由于不同的共轭类是不交的，因此得到

$$\begin{aligned}|G| &= |\overline{a}_1|+|\overline{a}_2|+\cdots+|\overline{a}_k|+|\overline{a}_{k+1}|+\cdots+|\overline{a}_{k+l}|\\ &= |\overline{a}_1|+|\overline{a}_2|+\cdots+|\overline{a}_k|+l.\end{aligned}$$

又由定理 3.30 有 $|\overline{a}_j|=[G:N(a_j)]$，$j=1,2,\cdots,k$，代入上式得

$$|G| = |C| + [G:N(a_1)] + [G:N(a_2)] + \cdots + [G:N(a_k)].$$

∎

【例 3.32】 设群 G 的阶为 p^s，$s\in Z^+$，p 是素数. 证明 G 的中心至少含两个元素.

证 由群的分类方程有

$$|G| = |C| + [G:N(a_1)] + [G:N(a_2)] + \cdots + [G:N(a_k)],$$

其中 $a_1,a_2,\cdots,a_k$ 是至少含 2 个元素的共轭类的代表. 根据 Lagrange 定理，对于 $i=1,2,\cdots,k$，$[G:N(a_i)]$ 是 p^s 的因子，因此有

$$[G:N(a_i)]=p^t(1\leqslant t\leqslant s)\text{ 或}[G:N(a_i)]=1.$$

若 $[G:N(a_i)]=1$，由定理 3.30 知 $|\overline{a}_i|=1$，即 $\overline{a}_i=\{a_i\}$，与 a_i 的定义矛盾. 所以必有 $[G:N(a_i)]=p^t$，$1\leqslant t\leqslant s$. 这就推出 $p\mid[G:N(a_i)]$.

考察 G 的分类方程，$p\mid|G|$，且 $\forall i=1,2,\cdots,k$，$p\mid[G:N(a_i)]$，必有 $p\mid|C|$. 这就证明 $|C|>1$. ∎

§ 3.6 正规子群和商群

G 是群，H 是 G 的子群，任给群 G 中的元素 a，一般说来 $Ha\neq$

aH.但对一些特殊的子群,它的左陪集和右陪集是相等的.

定义 3.21　G是群,H是G的子群,若$\forall a \in G$都有$Ha = aH$,则称H是G的**正规子群**①,记作$H \trianglelefteq G$.

【例 3.33**】**

(1) 群G的两个平凡子群G和$\{e\}$都是G的正规子群.因为$\forall a \in G$有$a\{e\} = \{e\}a$和$aG = Ga$.

(2) 群G的中心C是G的正规子群.

(3) 循环群的所有子群都是正规子群,因为循环群是Abel群.

(4) S_3的子群中有三个正规子群:$\{(1)\}$,S_3和$\{(1),(123),(132)\}$,其余三个不是正规子群.

下面给出关于正规子群的判定定理.

定理 3.32　N是群G的子群,则下列条件互相等价

(1) $N \trianglelefteq G$,

(2) $\forall g \in G$有$gNg^{-1} = N$,

(3) $\forall g \in G, \forall n \in N$有$gng^{-1} \in N$.

证　(1) $\Rightarrow$ (2).

$$N \trianglelefteq G \Rightarrow \forall g \in G \text{ 有 } gN = Ng$$
$$\Rightarrow \forall g \in G \text{ 有 } gNg^{-1} = Ngg^{-1} = N$$

(2) $\Rightarrow$ (3).

$$\forall g \in G,\ \forall n \in N,\ gng^{-1} \in gNg^{-1}$$
$$\Rightarrow \forall g \in G,\ \forall n \in N,\ gng^{-1} \in N$$

(3) $\Rightarrow$ (1).任取ng,

$ng \in Ng \Rightarrow n \in N \wedge g \in G \Rightarrow n \in N \wedge g^{-1} \in G$

$\Rightarrow g^{-1}n(g^{-1})^{-1} \in N \Rightarrow g^{-1}ng \in N$

$\Rightarrow \exists\, n_1 \in N(g^{-1}ng = n_1) \Rightarrow \exists\, n_1 \in N(ng = gn_1) \Rightarrow ng \in gN$;

任取gn,

① 正规子群也叫做不变子群.

$$gn \in gN \Rightarrow g \in G \wedge n \in N \Rightarrow gng^{-1} \in N$$
$$\Rightarrow \exists\, n_1 \in N(gng^{-1} = n_1) \Rightarrow \exists\, n_1 \in N(gn = n_1 g) \Rightarrow gn \in Ng.$$

综上所述，$\forall g \in G$ 有 $gN = Ng$，所以 $N \trianglelefteq G$. ▮

【例 3.34】 H 是群 G 的子群，$|H| = n$，若 H 是唯一的 n 阶子群，则 H 是 G 的正规子群.

证 任取 $g \in G$，由例 3.11 可知 $gHg^{-1} \leqslant G$. 令 φ: $H \to gHg^{-1}$，$\varphi(h) = ghg^{-1}$，$\forall h \in H$. 易证 φ 是一个双射，所以 $gHg^{-1} \approx H$，即 $|gHg^{-1}| = |H| = n$. 由于 G 中只有一个 n 阶子群，必有 $gHg^{-1} = H$. 由定理 3.32 得 $H \trianglelefteq G$. ▮

【例 3.35】 设 G 是群，$H \leqslant G$，若$[G : H] = 2$，则 H 是 G 的正规子群.

证 $H \leqslant G$ 且$[G : H] = 2$. 将 G 按 H 的右陪集分解可得 $G = H \cup Hg$，$\forall g \notin H$. 由于 $H \cap Hg = \varnothing$，则有

$$Hg = G - H, \forall g \notin H.$$

同理可证 $gH = G - H$，$\forall g \notin H$.

任取 $x \in G$，若 $x \in H$，则 $Hx = H = xH$；若 $x \notin H$，则有 $Hx = G - H = xH$. 从而有 $H \trianglelefteq G$.

【例3.36】 $G = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$，

则 G 关于矩阵乘法构成一个群. 它的子群除了两个平凡子群外还有：

$$H_1 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$

$$H_2 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\},$$

$$H_3 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\},$$

$$H_4 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}.$$

G 的子群格如图 3.4 所示. 两个平凡子群是 G 的正规子群. H_1 是唯一的二阶子群，根据例 3.34 的结论，H_1 是 G 的正规子群. H_2,H_3,H_4 在 G 中的指数都是 2，由例 3.35 的结论，它们也都是 G 的正规子群. 尽管群 G 不是 Abel 群，因为

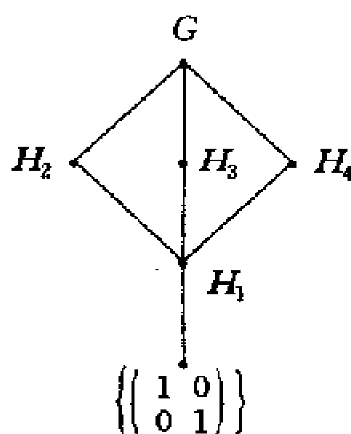


图 3.4

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

但它的所有子群都是正规子群.

定义 3.22　G 是群，H 是 G 的正规子群，令

$$G/H = \{Hg \mid g \in G\}$$

是 H 在 G 中的所有的右陪集构成的集合，在 G/H 上定义运算$\circ$，对任意的 $Ha, Hb \in G/H$ 有

$$Ha \circ Hb = Hab,$$

则 G/H 关于$\circ$运算构成一个群，称为 G 的**商群**.

为了保证商群定义的正确性，必须首先验证$\circ$运算是良定义的，与陪集代表元素的选择无关. 换句话说，若 $Hx = Ha$, $Hy = Hb$，则有

$$Hx \circ Hy = Ha \circ Hb.$$

证　设 $Hx = Ha$, $Hy = Hb$. 根据定理 3.22 可知 $x \in Ha$ 和 $y \in Hb$. 必存在 h_1 和 $h_2 \in H$ 使得 $x = h_1 a, y = h_2 b$. 又由于 H 是 G 的正规子群，所以推出

$$\begin{aligned} Hx \circ Hy &= Hxy = Hh_1 a h_2 b = Hh_1 (a h_2 a^{-1}) ab \\ &= Hh_1 h_2' ab = Hab = Ha \circ Hb. \end{aligned}$$

易见$\circ$运算是 G/H 上可结合的运算，因为对任意的 $Ha, Hb, Hc \in G/H$ 有

$$(Ha\circ Hb)\circ Hc = Hab\circ Hc = H(ab)c$$
$$= Ha(bc) = Ha\circ Hbc = Ha\circ(Hb\circ Hc).$$

$H = He$ 是关于$\circ$运算的单位元，因为对任意的 $Ha \in G/H$ 有

$$Ha\circ He = Hae = Ha \text{ 和 } He\circ Ha = Hea = Ha.$$

对任意的 $Ha \in G/H$，Ha^{-1} 是 Ha 关于$\circ$运算的逆元，因为有

$$Ha\circ Ha^{-1} = Haa^{-1} = He = H$$

和

$$Ha^{-1}\circ Ha = Ha^{-1}a = He = H.$$

这就证明了 G/H 关于$\circ$运算构成一个群. ∎

【例3.37】 $G = \langle Z, +\rangle$ 是整数加群，令

$$3Z = \{3k \mid k \in Z\},$$

则 $3Z$ 是 G 的正规子群. G 的商群

$$G/3Z = \{\bar{0}, \bar{1}, \bar{2}\},$$

表 3.6

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

其中 $\bar{i} = \{3k + i \mid k \in Z\}$，$G/3Z$ 上的运算如表 3.6 所示. 易见 $G/3Z \cong Z_3$. 从同构的意义上说，$G/3Z$ 就是 Z_3.

如果把群 G 看作代数系统 $\langle G, \cdot, ^{-1}, e\rangle$，那么 G 的商群 G/H 就是这个代数系统的商代数. 我们只需验证由 H 的右陪集作为等价类所导出的等价关系是 G 上的同余关系.

令 R 是上述的等价关系，$\forall a,b \in G$ 有

$$aRb \Leftrightarrow Ha = Hb \Leftrightarrow ab^{-1} \in H.$$

设 $a,b,c,d \in G$，由于 H 是 G 的正规子群，则

$$aRb \wedge cRd \Rightarrow ab^{-1} \in H \wedge cd^{-1} \in H$$
$$\Rightarrow \exists h_1 \in H(ab^{-1} = h_1) \wedge \exists h_2 \in H(cd^{-1} = h_2).$$

所以

$$ac(bd)^{-1} = a(cd^{-1})b^{-1} = ah_2b^{-1} = ab^{-1}h'_2 = h_1h'_2 \in H.$$

这就证明了 $acRbd$，R 关于 G 中二元运算具有置换性质. 此外

$$aRb \Rightarrow \exists h_1 \in H(ab^{-1} = h_1)$$
$$\Rightarrow \exists h_1 \in H(a^{-1} = b^{-1}h_1^{-1}),$$

所以

$$a^{-1}b = b^{-1}h_1^{-1}b \in H.$$

从而推出 $a^{-1}Rb^{-1}$，R 关于 G 中求逆运算具有置换性质，R 是代数系统 $\langle G, \cdot, ^{-1}, e\rangle$ 的同余关系.

【例 3.38】 G 为有限 Abel 群，$|G| = n$，p 是素数且 $p|n$. 证明 G 中存在 p 阶元.

证 对 n 进行归纳.

$n = 2$ 命题显然为真.

假设对一切 $m < n$ 命题为真，考虑 n 阶群 G，取 $a \in G, a \neq e$，则 $|a|\,|n$.

若 $p\,|\,|a|$，则 $a^{\frac{|a|}{p}}$ 是 G 中的 p 阶元.

若 $p \nmid |a|$，令 $H = \langle a \rangle$. 因为 G 为 Abel 群，则 H 是 G 的正规子群. 考虑 G 的商群 G/H，令 G/H 的阶是 m，则 $m = [G : H] < n$. 由 Lagrange 定理有

$$n = m \cdot |H|, \quad |H| = |a|.$$

$p|n$，但 $p \nmid |H|$，p 是素数，必有 $p|m$. 由归纳假设，G/H 中必存在 p 阶元.

设 G/H 中的 p 阶元为 Hb，则有

$$(Hb)^p = H \Rightarrow Hb^p = H \Rightarrow b^p \in H = \langle a \rangle \Rightarrow b^p = a^t.$$

因此有

$$(b^p)^{|a|} = (a^{|a|})^t = e \Rightarrow (b^{|a|})^p = e.$$

这就推出 $b^{|a|}$ 的阶为 p 或 1. 假设 $b^{|a|}$ 的阶是 1，则 $b^{|a|} = e$，必有 $(Hb)^{|a|} = H$，与 $p \nmid |a|$ 矛盾. 从而证明了 $b^{|a|}$ 是 p 阶元. ∎

§3.7 群的同态与同构

定义 3.23 设 G_1 和 G_2 是群，φ 是 G_1 到 G_2 的映射. 若对于任意的 $x, y \in G$，有

$$\varphi(xy) = \varphi(x)\,\varphi(y),$$

则称 φ 是群 G_1 到 G_2 的**同态映射**，简称**同态**.

可以证明，若把群看作是具有一个可结合的二元运算、一个求逆元的一元运算和一个零元运算(二元运算的单位元 e) 的代数系统，则上述定义的群同态就是代数系统 $\langle G_1, \cdot, ^{-1}, e_1\rangle$ 到 $\langle G_2, \cdot, ^{-1}, e_2\rangle$ 的同态，为此必须验证：

$$\varphi(e_1) = e_2,$$

$$\varphi(x^{-1}) = \varphi(x)^{-1}, \qquad \forall x \in G_1.$$

由

$$\varphi(e_1)\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1)$$

可知 $\varphi(e_1)$ 是 G_2 中的幂等元，由例 3.4 可知群的单位元是唯一的幂等元，所以 $\varphi(e_1) = e_2$.

任取 $x \in G_1$ 有

$$\varphi(x)\varphi(x^{-1}) = \varphi(e_1) = e_2,\ \varphi(x^{-1})\varphi(x) = \varphi(e_1) = e_2.$$

$\varphi(x^{-1})$ 是 $\varphi(x)$ 的逆元，由逆元的唯一性可得 $\varphi(x^{-1}) = \varphi(x)^{-1}$.

根据一般代数系统的满同态、单同态和同构的定义可直接得到群的满同态、单同态和同构的定义. 如果群 G_1 到 G_2 存在满同态 φ，可以记作 $G_1 \overset{\varphi}{\sim} G_2$，如果 φ 是 G_1 到 G_2 的同构，则记作 $G_1 \overset{\varphi}{\cong} G_2$.

【例 3.39】 (1) 证明群 $G_1 = \langle R, +\rangle$ 和 $G_2 = \langle R^+, \cdot\rangle$ 是同构的；

(2) 证明不存在群 $G_1 = \langle Q^*, \cdot\rangle$ 到 $G_2 = \langle Q, +\rangle$ 的同构，其中 $Q^* = Q - \{0\}$，$\cdot$ 为普通乘法.

证 (1) 令 $\varphi: R \to R^+$，$\varphi(x) = e^x$，$\forall x \in R$，则 φ 是双射，且 $\forall x, y \in R$ 有

$$\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y).$$

(2) 假设 $\varphi: Q^* \to Q$ 是 G_1 到 G_2 的同构，则 $\varphi(1) = 0$.

由此得

$$\varphi(-1)+\varphi(-1)=\varphi((-1)(-1))=\varphi(1)=0.$$

于是有 $\varphi(-1)=0$，与 φ 是双射矛盾. ∎

【例 3.40】 (Cayley 定理)

任何群 G 都同构于 G 的一个变换群.

证 回顾例 3.18，定义 $f_a: G\to G$, $f_a(x)=ax, \forall x\in G$. 令 $H=\{f_a|a\in G\}$，则 H 是 G 上的一个变换群. 下面证明 G 同构于 H.

令 $\varphi: G\to H$, $\varphi(a)=f_a$, $\forall a\in G$. 则 $\forall a,b\in G$,

$$\varphi(ab)=f_{ab}=f_af_b=\varphi(a)\varphi(b),$$

φ 是 G 到 H 的同态.

假设 $\varphi(a)=\varphi(b)$, $a,b\in G$，则 $f_a=f_b$，即 $\forall x\in G$ 有 $f_a(x)=f_b(x)$. 从而有 $f_a(e)=f_b(e)$，即 $a=b$. φ 是单同态.

对任意的 $f_a\in H$，$\exists\ a\in G$ 使 $\varphi(a)=f_a$，φ 是满同态.

综合以上结果有 $G\overset{\varphi}{\cong}H$. 易见 $H\leqslant E(G)$，$E(G)$ 是 G 的一一变换群.

例如 $G=\langle Z_3,\oplus\rangle$，其中 $\oplus$ 为模 3 加法，则有

f_0: $0\mapsto 0, 1\mapsto 1, 2\mapsto 2$;

f_1: $0\mapsto 1, 1\mapsto 2, 2\mapsto 0$;

f_2: $0\mapsto 2, 1\mapsto 0, 2\mapsto 1$.

$\{f_0,f_1,f_2\}$ 是 G 上的变换群，且与 G 同构.

定义 3.24 设 $\varphi: G_1\to G_2$ 是群 G_1 到 G_2 的同态，令

$$\ker\varphi=\{x|x\in G\wedge\varphi(x)=e_2\},$$

称 $\ker\varphi$ 为 φ 的核.

【例 3.41】 (1) 设 G_1 是整数加群，G_2 为模 n 整数加群，令 $\varphi: Z\to Z_n$, $\varphi(x)=(x)\bmod n$，则 φ 是 G_1 到 G_2 的满同态，且 $\ker\varphi=\{nk\,|\,k\in Z\}=nZ$.

(2) 设 G 是群，自然映射 $g: G\to G/H$, $g(x)=Hx$, $\forall x\in G$, 是 G 到 G 的商群 G/H 的满同态，且

$$\ker g = \{x \mid x \in G \wedge x \in H\} = H.$$

除了一般代数系统的同态性质之外，群同态还有一些特殊的性质. 请看下面的定理.

定理 3.33　设 φ 是群 G_1 到 G_2 的同态，则 φ 为单同态当且仅当

$$\ker\varphi = \{e_1\}.$$

证　必要性. 假设存在 $a \in \ker\varphi$, $a \neq e_1$，则有 $\varphi(a) = e_2$, $\varphi(e_1) = e_2$，与 φ 是单同态矛盾.

充分性. 若 $\varphi(a) = \varphi(b)$, $a,b \in G$，则有

$$\varphi(a)\varphi(b)^{-1} = e_2 \Rightarrow \varphi(ab^{-1}) = e_2 \Rightarrow ab^{-1} \in \ker\varphi$$

$$\Rightarrow ab^{-1} = e_1 \Rightarrow a = b.$$

这就推出 φ 是单射的，所以 φ 是单同态. ∎

定理 3.34　$G_1 = \langle a \rangle$ 是循环群，φ 是 G_1 到 G_2 的满同态，则 G_2 也是循环群.

证　任取 $x \in G_2$，由于 φ 是满射，必存在 $a^t \in G_1$，使 $\varphi(a^t) = x$，从而有

$$x = \varphi(a^t) = \varphi(a)^t,$$

$\varphi(a)$ 是 G_2 的生成元，$G_2 = \langle \varphi(a) \rangle$. ∎

定理 3.35　设 φ 是群 G_1 到 G_2 的同态.

(1) 若 H 是 G_1 的子群，则 $\varphi(H)$ 是 G_2 的子群.

(2) 若 H 是 G_1 的正规子群，且 φ 是满同态，则 $\varphi(H)$ 是 G_2 的正规子群.

证　(1) $\varphi \upharpoonright H: H \to G_2$ 是同态. 由定理 1.7 可知 $\varphi(H) = \varphi \upharpoonright H(H)$ 是 G_2 的子代数，所以 $\varphi(H) \leqslant G_2$.

(2) 由(1)可知 $\varphi(H) \leqslant G_2$. 任取 $x \in G_2$, $\varphi(h) \in \varphi(H)$，因为 φ 是满射，必存在 $a \in G_1$ 使得 $\varphi(a) = x$，从而有

$$x\varphi(h)x^{-1} = \varphi(a)\varphi(h)\varphi(a)^{-1} = \varphi(aha^{-1}).$$

由于 $H \trianglelefteq G_1$, $aha^{-1} \in H$，所以 $\varphi(aha^{-1}) \in \varphi(H)$. 根据正规子群的判定定理有 $\varphi(H) \trianglelefteq G_2$. ∎

定理 3.36　设 φ 是群 G_1 到 G_2 的同态，则

(1) $\ker\varphi$ 是 G_1 的正规子群；

(2) $\forall a,b \in G_1, \varphi(a) = \varphi(b) \Leftrightarrow a\ker\varphi = b\ker\varphi$.

证　(1) $e_1 \in \ker\varphi$, $\ker\varphi$ 非空. $\forall a,b \in \ker\varphi$ 有

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_2e_2^{-1} = e_2,$$

所以 $ab^{-1} \in \ker\varphi$. 由子群判定定理有 $\ker\varphi \leqslant G_1$.

$\forall x \in G_1$, $\forall a \in \ker\varphi$ 有

$$\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x)^{-1} = \varphi(x)e_2\varphi(x)^{-1} = e_2,$$

所以 $xax^{-1} \in \ker\varphi$, 由定理 3.32 知 $\ker\varphi \trianglelefteq G_1$.

(2) $\forall a,b \in G_1$ 有

$$\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)^{-1}\varphi(b) = e_2 \Leftrightarrow \varphi(a^{-1}b) = e_2$$

$$\Leftrightarrow a^{-1}b \in \ker\varphi \Leftrightarrow a\ker\varphi = b\ker\varphi.$$ ∎

定理 3.37　(群同态基本定理) 设 G 是群，H 是 G 的正规子群，则 G 的商群 G/H 是 G 的同态像. 若 G' 是 G 的同态像，$G \overset{\varphi}{\sim} G'$，则

$$G/\ker\varphi \cong G'.$$

证　G 的商群 G/H 是 G 的商代数. 由定理 1.11 知自然映射是从 G 到 G/H 的满同态映射，因此 G/H 是 G 的同态像.

设 $G \overset{\varphi}{\sim} G'$，即 φ 是 G 到 G' 的满同态，由定理 3.36 有 $\ker\varphi \trianglelefteq G$，且 $G/\ker\varphi = \{a\ker\varphi \mid a \in G\}$.

在 G 上定义二元关系 $\sim$，$\forall a,b \in G$ 有

$$a \sim b \Leftrightarrow \varphi(a) = \varphi(b).$$

则由定理 1.10 知 $\sim$ 是 G 上的同余关系，且 G 的商代数 $G/\sim = \{[a] \mid a \in G\}$. 根据定理 3.36 可知对任意 $a,b \in G$ 有

$$[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow a\ker\varphi = b\ker\varphi,$$

且有

$$[a] \cdot [b] = [ab], \quad a\ker\varphi \cdot b\ker\varphi = ab\ker\varphi.$$

所以 $G/\ker\varphi$ 就是 $G/\sim$. 由同态基本定理(定理 1.12) 可知 $G/\sim \cong G'$，

从而有 $G/\ker\varphi \cong G'$.

∎

由以上证明不难看出，群同态基本定理就是一般代数系统同态基本定理的特例.

【例 3.42】 设 φ 为群 G_1 到 G_2 的同态，则

$$\varphi \text{为零同态} \Leftrightarrow \ker\varphi = G_1.$$

证 φ 为零同态 $\Leftrightarrow \forall x(x \in G_1 \to \varphi(x) = e_2)$

$\Leftrightarrow \forall x(x \in G_1 \to x \in \ker\varphi) \Leftrightarrow G_1 \subseteq \ker\varphi \Leftrightarrow \ker\varphi = G_1$. ∎

【例 3.43】 设 φ 是群 G_1 到 G_2 的同态，若 G_1 是单群(G_1 无非平凡的正规子群)，则 φ 为单同态或零同态.

证 假设 φ 不是单同态. 由定理 3.33 可知 $\ker\varphi \neq \{e_1\}$. 由于 G_1 是单群且 $\ker\varphi \lhd G_1$(定理 3.36)，必有 $\ker\varphi = G_1$. 这就证明了 φ 是零同态.

∎

【例 3.44】 设 G_1, G_2 分别为 m, n 阶循环群，证明 G_2 是 G_1 的同态像当且仅当 $n|m$.

证 设 $G_1 = \langle a \rangle, G_2 = \langle b \rangle$.

充分性. 令 φ: $G_1 \to G_2$, $\varphi(a^i) = b^i$, $i = 0, 1, \cdots, m-1$. 由于 $n|m$，必有 $a^i = a^j \Rightarrow m|(i-j) \Rightarrow n|(i-j) \Rightarrow b^i = b^j$，$\varphi$ 是 G_1 到 G_2 的映射. 易见 φ 是满射. $\forall a^i, a^j \in G_1$ 有

$$\varphi(a^i a^j) = \varphi(a^{i+j}) = b^{i+j} = b^i b^j = \varphi(a^i)\varphi(a^j),$$

因此 $G_1 \overset{\varphi}{\sim} G_2$，$G_2$ 是 G_1 的同态像.

必要性. 设 $G_1 \overset{\varphi}{\sim} G_2$，由同态基本定理有 $G_2 \cong G_1/\ker\varphi$，即 $|G_2| = |G_1/\ker\varphi|$，从而有 $[G_1 : \ker\varphi] = |G_1/\ker\varphi| = n$. 由 Lagrange 定理可知，$[G_1 : \ker\varphi]$ 整除 $|G_1|$，这就推出 $n|m$.

∎

【例 3.45】 设 φ 是群 G_1 到 G_2 的满同态，$\ker\varphi = K$，令

$$S_1 = \{H | H \leqslant G_1 \land K \subseteq H\},$$
$$S_2 = \{H | H \leqslant G_2\}.$$

则存在双射 f: $S_1 \to S_2$, $f(H) = \varphi(H)$, $\forall H \in S_1$.

证 任取 $H \in S_1$，由定理 3.35 知 $\varphi(H) \leqslant G_2$.

显然 $H \subseteq \varphi^{-1}(\varphi(H))$. 任取 $a \in \varphi^{-1}(\varphi(H))$，则 $\varphi(a) \in \varphi(H)$，必存在 $b \in H$ 使得 $\varphi(a) = \varphi(b)$. 根据定理 3.36 知 $a\ker\varphi = b\ker\varphi$，从而 $a \in b\ker\varphi = bK$. 而由 $b \in H$ 知 $bK \subseteq H$，所以有 $a \in H$. 这就推出了 $H = \varphi^{-1}(\varphi(H))$.

假设 $f(H_1) = f(H_2)$，$H_1, H_2 \in S_1$，则有

$$f(H_1) = f(H_2) \Rightarrow \varphi(H_1) = \varphi(H_2)$$
$$\Rightarrow \varphi^{-1}(\varphi(H_1)) = \varphi^{-1}(\varphi(H_2)) \Rightarrow H_1 = H_2.$$

所以 f 是单射的.

任取 $H \in S_2$，则 $\varphi^{-1}(H) \subseteq G_1$，且 $e_1 \in \varphi^{-1}(H)$，$\varphi^{-1}(H)$ 非空. 任取 $a, b \in \varphi^{-1}(H)$，则

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}.$$

$\varphi(a)$，$\varphi(b) \in H$，H 是 G_2 的子群，必有 $\varphi(ab^{-1}) \in H$，从而有 $ab^{-1} \in \varphi^{-1}(H)$. 这就证明 $\varphi^{-1}(H) \leqslant G_1$. 易见 $K \subseteq \varphi^{-1}(H)$，因此有 $\varphi^{-1}(H) \in S_1$，$f(\varphi^{-1}(H)) = H$. f 是满射的. ∎

【例 3.46】 G 是群，$N \trianglelefteq G$，$K \leqslant G$，证明

(1) $NK \leqslant G$，$N \trianglelefteq NK$；

(2) $N \cap K \trianglelefteq K$；

(3) $NK/N \cong K/(N \cap K)$.

证 (1) $e \in NK$，NK 非空. 任取 $n_1k_1, n_2k_2 \in NK$，则

$$(n_1k_1)(n_2k_2)^{-1} = n_1k_1k_2^{-1}n_2^{-1} = n_1k_1n'_2k_2^{-1} = n_1n''_2k_1k_2^{-1},$$

即 $(n_1k_1)(n_2k_2)^{-1} \in NK$，所以 $NK \leqslant G$.

显然 N 是 NK 的子群，任取 $x \in NK$，必有 $x \in G$. 由于 $N \trianglelefteq G$，$xN = Nx$，所以 $N \trianglelefteq NK$.

(2) 显然 $N \cap K \leqslant K$，任取 $x \in N \cap K$，$k \in K$ 有

$$kxk^{-1} = n'kk^{-1} \in N,$$
$$kxk^{-1} \in K（因为 k, x, k^{-1} 都属于 K），$$

所以 $kxk^{-1} \in N \cap K$，从而推出 $N \cap K \trianglelefteq K$.

(3) 令 φ: $NK \to K/(N \cap K)$，

$$\varphi(nk) = (N \cap K)k, \forall nk \in NK.$$

易证 φ 是 NK 到 $K/(N \cap K)$ 的映射. 任取 $(N \cap K)k \in K/(N \cap K)$，则存在 $nk \in NK$，使得 $\varphi(nk) = (N \cap K)k$，$\varphi$是满射.

任取 $n_1k_1, n_2k_2 \in NK$，

$$\varphi(n_1k_1n_2k_2) = \varphi(n_1n'_2k_1k_2) = (N \cap K)k_1k_2$$
$$= (N \cap K)k_1(N \cap K)k_2 = \varphi(n_1k_1)\varphi(n_2k_2),$$

φ是 NK 到 $K/(N \cap K)$ 的满同态，且

$$\ker\varphi = \{nk \mid (N \cap K)k = N \cap K\} = \{nk \mid k \in N \cap K\}$$
$$= \{nk \mid k \in N\} = N.$$

由同态基本定理有 $NK/N \cong K/(N \cap K)$. ∎

【例 3.47】 G 是群，$H \trianglelefteq G$，$K \trianglelefteq G$，$H \subseteq K$，则

$$G/K \cong (G/H)/(K/H).$$

证 定义 φ: $G/H \to G/K$，$\varphi(Ha) = Ka$，$\forall Ha \in G/H$. 则有

$$Ha = Hb \Rightarrow ab^{-1} \in H \Rightarrow ab^{-1} \in K \Rightarrow Ka = Kb,$$

φ是良定义的. 任取 $Ka \in G/K$，则 $Ha \in G/H$，使得 $\varphi(Ha) = Ka$，所以 φ是满射的.

对任意的 Ha，$Hb \in G/H$ 有

$$\varphi(Ha\ Hb) = \varphi(Hab) = Kab = Ka\ Kb = \varphi(Ha)\varphi(Hb),$$

因此 φ是满同态，且

$$\ker\varphi = \{Ha \mid a \in K\} = K/H.$$

由同态基本定理有 $G/K \cong (G/H)/(K/H)$. ∎

下面考虑群的自同态和自同构.

定义 3.25 设 G 是一个群，G 到 G 的同态称为 G 的**自同态**，G 到 G 的同构称为**自同构**. G 的全部自同态的集合记作 End$G$，G 的全部自同构的集合记作 Aut$G$.

定理 3.38　G 是群，则 End$G$ 关于映射的合成运算构成一个独异点，Aut$G$ 关于映射的合成运算构成一个群.

证　任取 $\sigma,\tau \in \text{End}G$，则 $\sigma,\tau \in G^G$，且 $\sigma\tau \in G^G$. 对任意的 $a,b \in G$ 有

$$\begin{aligned}\sigma\tau(ab) &= \sigma(\tau(ab)) = \sigma(\tau(a)\tau(b)) = \sigma(\tau(a))\sigma(\tau(b)) \\ &= \sigma\tau(a)\sigma\tau(b).\end{aligned}$$

这就证明 $\sigma\tau \in \text{End}G$. 恒等映射 I_G 是 End$G$ 中的单位元，映射的合成满足结合律，所以 End 关于映射的合成运算构成半群和独异点.

易见 Aut$G$ 关于映射的合成构成独异点，对任意 $\sigma \in \text{Aut}G$，σ^{-1} 是 σ 的逆元，所以 Aut$G$ 关于映射的合成运算构成群，称为 G 的**自同构群**. ∎

定义 3.26　G 是群，$x \in G$，令 φ_x: $G \to G$，$\varphi_x(a) = xax^{-1}$，$\forall a \in G$. 易证 φ_x 是 G 的自同构，称为**内自同构**. G 的所有内自同构的集合记作 Inn$G$.

定理 3.39　G 是群，则 $\text{Inn}G \trianglelefteq \text{Aut}G$.

证　恒等映射 $I_G = \varphi_e$，Inn$G$ 非空. 任取 $y \in G$，则 $\forall a \in G$ 有 $\varphi_y^{-1}(a) = y^{-1}ay$.

任取 $\varphi_x,\varphi_y \in \text{Inn}G$，则 $\forall a \in G$ 有

$$\begin{aligned}\varphi_x\varphi_y^{-1}(a) &= \varphi_x(y^{-1}ay) = xy^{-1}ayx^{-1} \\ &= (xy^{-1})a(xy^{-1})^{-1} = \varphi_{xy^{-1}}(a).\end{aligned}$$

这说明 $\varphi_x\varphi_y^{-1} \in \text{Inn}G$，从而有 $\text{Inn}G \leqslant \text{Aut}G$.

任取 $\sigma \in \text{Aut}G$，$\varphi_x \in \text{Inn}G$，则 $\forall a \in G$ 有

$$\begin{aligned}&\sigma\varphi_x\sigma^{-1}(a) = \sigma(\varphi_x(\sigma^{-1}(a))) = \sigma(x\sigma^{-1}(a)x^{-1}) \\ &= \sigma(x)\sigma(\sigma^{-1}(a))\sigma(x)^{-1} = \sigma(x)a\sigma(x)^{-1} = \varphi_{\sigma(x)}(a).\end{aligned}$$

这就推出 $\sigma\varphi_x\sigma^{-1} \in \text{Inn}G$，因此有 $\text{Inn}G \trianglelefteq \text{Aut}G$. ∎

【例 3.48】　$G = \langle Z_3, \oplus \rangle$，$\oplus$ 为模 3 加法. G 上的自同态有三个，即

$\varphi_p: Z_3 \to Z_3$, $\varphi_p(x) = (px)\bmod 3$, $p = 0,1,2$, 其中

φ_0: $0 \mapsto 0$, $1 \mapsto 0$, $2 \mapsto 0$, 零同态.

φ_1: $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 2$, 恒等映射,同构.

φ_2: $0 \mapsto 0$, $1 \mapsto 2$, $2 \mapsto 1$, 同构.

$\mathrm{End}G = \{\varphi_0,\varphi_1,\varphi_2\}$, $\mathrm{Aut}G = \{\varphi_1,\varphi_2\}$, $\mathrm{Inn}G = \{\varphi_1\}$.

【例 3.49】 设 G 是群,H 是 G 的子群,则 H 是 G 的正规子群当且仅当对任意的 $\varphi_x \in \mathrm{Inn}G$ 都有 $\varphi_x(H) \subseteq H$.

证 必要性. $H \trianglelefteq G$,根据定理 3.32 可知对任意的 $x \in G, h \in H$ 都有 $xhx^{-1} \in H$.

任取 $a \in \varphi_x(H)$,则 $\exists\, h \in H$ 使得 $a = xhx^{-1}$,必有 $a \in H$,因此 $\varphi_x(H) \subseteq H$.

充分性. 任取 $x \in G$, $h \in H$,有 $xhx^{-1} \in \varphi_x(H)$,由于 $\varphi_x(H) \subseteq H$, $xhx^{-1} \in H$,所以有 $H \trianglelefteq G$. ∎

【例 3.50】 设 φ 为群 G 的自同构,

(1) $\forall x \in G$,若 x 的阶存在,则 $|x| = |\varphi(x)|$;

(2) 若 $H \leqslant G$,则 $H \cong \varphi(H)$;

(3) 若 $H \trianglelefteq G$,则 $\varphi(H) \trianglelefteq G$,且 $G/H \cong G/\varphi(H)$.

证 (1) $\forall x \in G$,若 $|x| = n$,则有

$$\varphi(x)^n = \varphi(x^n) = \varphi(e) = e,$$

由定理 3.8 知 $|\varphi(x)|$ 是 n 的因子.

下面证明 φ^{-1} 也是 G 的自同构. 显然 φ^{-1} 为双射. 任取 $x, y \in G$,必存在 $a, b \in G$,使得 $\varphi(a) = x, \varphi(b) = y$,因此可得

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

根据上面的证明可知 $|\varphi^{-1}(\varphi(x))|$ 是 $|\varphi(x)|$ 的因子,这就推出 $n \mid |\varphi(x)|$.

综合上面的结果有 $|x| = |\varphi(x)|$.

(2) 已知 $\varphi: G \to G$ 是同构,则 $\varphi\restriction H: H \to \varphi(H)$ 是双射,也是同

态映射，所以有 $H \cong \varphi(H)$.

(3) 根据定理 3.35 可知 $\varphi(H) \lhd G$. 令 $g: G/H \to G/\varphi(H)$,

$$g(Ha) = \varphi(H)\varphi(a), \ \forall Ha \in G/H.$$

任取 $Ha, Hb \in G/H$，则有

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow \varphi(ab^{-1}) \in \varphi(H)$$
$$\Leftrightarrow \varphi(a)\varphi(b)^{-1} \in \varphi(H) \Leftrightarrow \varphi(H)\varphi(a) = \varphi(H)\varphi(b),$$

从而推出 g 是良定义的，也是单射的.

任取 $\varphi(H)b \in G/\varphi(H)$，则 $\varphi^{-1}(b) \in G$，且

$$g(H\varphi^{-1}(b)) = \varphi(H)\varphi(\varphi^{-1}(b)) = \varphi(H)b.$$

这就证明了 g 是满射的.

最后我们来验证 g 是 G/H 到 $G/\varphi(H)$ 的同态. 任取 $Ha, Hb \in G/H$，则有

$$g(Ha\ Hb) = g(Hab) = \varphi(H)\varphi(ab) = \varphi(H)\varphi(a)\varphi(b)$$
$$= \varphi(H)\varphi(a)\varphi(H)\varphi(b) = g(Ha)g(Hb).$$

g 是同构，于是 $G/H \cong G/\varphi(H)$. ∎

§3.8 群的直积

群的积代数就是群的直积. 下面考虑群的内直积.

定义 3.27 设 G 是群，K, L 是 G 的子群. φ: $K \times L \to KL$, $\varphi(\langle k, l\rangle) = kl, \forall k \in K, \forall l \in L$. 若 φ 是 $K \times L$ 到 G 的同构，则称 G 是 K 和 L 的**内直积**，记作 $G = K \times L$.

【例 3.51】 设 $G = \langle Z_6, \oplus\rangle$, $K = \{0,2,4\} = \langle 2\rangle$, $L = \{0,3\} = \langle 3\rangle$，则 K 和 L 都是 G 的子群.

$$K \times L = \{\langle 0,0\rangle, \langle 0,3\rangle, \langle 2,0\rangle, \langle 2,3\rangle, \langle 4,0\rangle, \langle 4,3\rangle\}$$
$$= \langle\langle 2,3\rangle\rangle,$$
$$KL = \{0,3,2,5,4,1\} = \langle 5\rangle,$$

易见 $K \times L$, KL 是同构的，所以 $G = K \times L$.

关于内直积有以下定理.

定理 3.40 设G是群,K和L是G的子群,则$G = K \times L$当且仅当下面的条件成立:

(1) $K \trianglelefteq G$, $L \trianglelefteq G$;

(2) $K \cap L = \{e\}$;

(3) $G = KL$.

证 必要性.令

$$K_1 = \{\langle k,e\rangle \mid k \in K\},$$
$$L_1 = \{\langle e,l\rangle \mid l \in L\},$$

易证K_1和L_1是$K \times L$的正规子群,且$K \times L = K_1L_1$.定义

$$\varphi: K \times L \to G,\ \varphi(\langle k,l\rangle) = kl,$$

则$\varphi(K_1) = K$,$\varphi(L_1) = L$.由于φ是同构,K和L是G的正规子群,且

$$\varphi(K_1) \cap \varphi(L_1) = K \cap L.$$

由于

$$\varphi^{-1}(\varphi(K_1) \cap \varphi(L_1)) \subseteq \varphi^{-1}(\varphi(K_1)) \cap \varphi^{-1}((\varphi(L_1)) = K_1 \cap L_1,$$

$K_1 \cap L_1 = \{\langle e,e\rangle\}$,所以

$$\varphi(K_1) \cap \varphi(L_1) \subseteq \varphi(K_1 \cap L_1) = \varphi(\{\langle e,e\rangle\}) = \{e\}.$$

这就证明了$K \cap L = \{e\}$.

易见$KL \subseteq G$.任取$x \in G$,由φ是同构可知必存在$k \in K$,$l \in L$使得$\varphi(\langle k,l\rangle) = x$且$x = kl \in KL$,于是有$G \subseteq KL$.综合这两方面的结果必有$G = KL$.

充分性.任取$k \in K$,$l \in L$,先证$kl = lk$,令

$$u = k^{-1}l^{-1}kl,$$

则由$K \trianglelefteq G$可知$l^{-1}kl = l^{-1}k(l^{-1})^{-1} \in K$,因此$u \in K$.又由$L \trianglelefteq G$知$k^{-1}l^{-1}k = k^{-1}l^{-1}(k^{-1})^{-1} \in L$,因此$u \in L$.由已知条件$K \cap L = \{e\}$得$u = e$,即$k^{-1}l^{-1}kl = e$,从而证得$kl = lk$.

令φ: $K \times L \to KL$, $\varphi(\langle k,l\rangle) = kl$, $\forall k \in K$, $l \in L$,则$\forall \langle k_1,l_1\rangle,\langle k_2,l_2\rangle \in K \times L$有

$$\varphi(\langle k_1,l_1\rangle\langle k_2,l_2\rangle) = \varphi(\langle k_1k_2,l_1l_2\rangle) = k_1k_2l_1l_2$$
$$=k_1l_1k_2l_2 = \varphi(\langle k_1,l_1\rangle)\varphi(\langle k_2,l_2\rangle).$$

φ是同态映射. 易见 φ是满同态.

$\forall k \in K, l \in L$ 有

$$\langle k,l\rangle \in \ker\varphi \Leftrightarrow kl = e \Leftrightarrow k = l^{-1} \Rightarrow k,l \in K \land k,l \in L$$
$$\Rightarrow k,l \in K \cap L \Rightarrow k = l = e,$$

所以 $\ker\varphi = \{\langle e,e\rangle\}$,由定理 3.33 知 φ为单同态. 这就证明 φ是 $K \times L$ 到 KL 的同构. 由 $G = KL$ 可知 φ是 $K \times L$ 到 G 的同构,所以 $G = K \times L$. ∎

【例 3.52】 设 G 是 pq 阶循环群,p 和 q 是不相等的素数,K 和 L 分别为 G 的 p 阶子群和 q 阶子群,则 $G = K \times L$.

证 K 和 L 也是循环群,令 $K = \langle a\rangle$, $L = \langle b\rangle$,则 $K \trianglelefteq G, L \trianglelefteq G$. 任取 $x \in K \cap L$,则 $|x| \mid p$, $|x| \mid q$. 又由于 $(p,q) = 1$,所以 $|x| = 1$,即 $K \cap L = \{e\}$.

$ab \in KL$,且 $|ab| = |a| \cdot |b| = pq$,因此 $KL = G$,由定理3.40, $G = K \times L$. ∎

定义 3.27 和定理 3.40 可以推广到 n 个子群的情况.

定义 3.28 设 G 是群,$G_1,G_2,\cdots,G_n$ 是 G 的子群. 设

$$\varphi: G_1 \times G_2 \times \cdots \times G_n \to G_1G_2\cdots G_n,$$
$$\varphi(\langle a_1,a_2,\cdots,a_n\rangle) = a_1a_2\cdots a_n, \forall a_i \in G_i,\ i = 1,2,\cdots,n.$$

若 φ是 $G_1 \times G_2 \times \cdots \times G_n$ 到 G 的同构,则称 G 是 $G_1,G_2,\cdots,G_n$ 的内直积,记作 $G = G_1 \times G_2 \times \cdots \times G_n$.

限于篇幅,略去证明,我们仅给出定理 3.41,它是定理 3.40 的推广形式.

定理 3.41 设 G 是群,$G_1,G_2,\cdots,G_n$ 是 G 的子群,则 $G = G_1 \times G_2 \times \cdots \times G_n$ 当且仅当以下条件成立:

(1) $G_i \trianglelefteq G$, $i = 1,2,\cdots,n$;

(2) $G_i \cap G_1G_2\cdots G_{i-1}G_{i+1}\cdots G_n = \{e\}$, $i = 1,2,\cdots,n$;

(3) $G = G_1G_2\cdots G_n$.

作为本章的结束，我们给出一个群的应用实例 —— 估计加法器的时间复杂性下界. 先定义 r- 电路.

定义 3.29 如果一个电路至多有 r 个输入，则称这个电路为 r-电路.

图 3.5 的电路就是一个 r- 电路，为了简便起见，假设在网络中的每个 r- 电路的延迟时间都是 1 个时间单位.

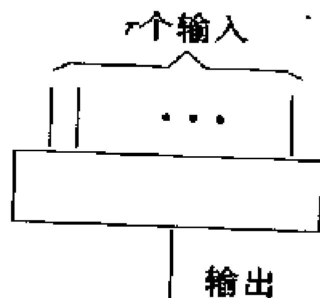


图 3.5

定理 3.42 用 r- 电路计算一个 m 元函数至少需要 $\lceil \log_r m \rceil$[①]个时间单位.

证 设计算 m 元函数需要 t 级 r- 电路，则有 $m \leqslant r^t$. 而 t 级电路的延迟时间为 t 个时间单位，故 $t \geqslant \lceil \log_r m \rceil$. ∎

令 $Z_n = \{0,1,\cdots,n-1\}$，考虑 Z_n 上的加法. 对任意的 $x \in Z_n$，x 的二进制表示有 m 位，其中第 i 位记作 $(x)_i$. 易见 Z_n 关于模 n 整数加法 $\oplus$ 构成群. $\forall x,y \in Z_n$，令 $-y$ 表示 y 的逆元，$x - y$ 表示 $x \oplus (-y)$，$x \otimes y$ 表示 $(xy)\mathrm{mod}\, n$，则

$$x \otimes Z_n = \{x \otimes z \mid z \in Z_n\}$$

是 Z_n 的子群. 因为 $0 = x \otimes 0 \in x \otimes Z_n$，$x \otimes Z_n$ 非空. 任取 $x \otimes z_1$，$x \otimes z_2 \in x \otimes Z_n$ 有

$$(x \otimes z_1) \oplus (x \otimes z_2) = x \otimes (z_1 \oplus z_2) \in x \otimes Z_n,$$

根据定理 3.11，$x \otimes Z_n$ 是 Z_n 的子群.

引理 设 $\langle Z_n, \oplus \rangle$ 是群，$x,y \in Z_n$，$i \in \{1,2,\cdots,m\}$. 如果 $\forall z \in Z_n$ 有 $(x \oplus z)_i = (y \oplus z)_i$，则对于任意的 $u \in (x-y) \otimes Z_n$ 有 $(u)_i = 0$.

证 $\forall z \in Z_n$，由 $(x \oplus z)_i = (y \oplus z)_i$ 得

① $\lceil x \rceil$ 表示大于等于 x 的最小整数.

$((x-y)\oplus z)_i=(x\oplus(-y)\oplus z)_i=((y-y)\oplus z)_i=(z)_i.$

任取 $u\in(x-y)\otimes Z_n$，则 $u=(x-y)\otimes z, z\in Z_n$. 若 $z=0$，则 $u=(x-y)\otimes 0=0,(u)_i=0.$

假设 $z=k(k=0,1,\cdots,n-2)$ 时有

$$(u)_i=((x-y)\otimes k)_i=0,$$

则当 $z=k+1$ 时有

$$u=(x-y)\otimes(k+1)=(x-y)\oplus((x-y)\otimes k),$$

从而得到

$$(u)_i=((x-y)\oplus((x-y)\otimes k))_i=((x-y)\otimes k)_i=0.$$

∎

定理 3.43　设 $\langle Z_n,\oplus\rangle$ 是群，若存在 $a\in Z_n, a\neq 0$，且 a 属于 Z_n 的每一个非平凡的子群，则对于任意的模 n 加法器 T 总存在着某个输入使得 T 至少依赖于输入的 $2\lceil\log_2 n\rceil$ 位.

证　由 $a\neq 0$ 可知存在 i 使得 $(a)_i\neq 0$. 下面证明 T 的第 i 位输出至少依赖于每个输入的 $\lceil\log_2 n\rceil$ 位.

假设 T 的第 i 位输出至多依赖于某个输入的 $\lceil\log_2 n\rceil-1$ 位. 由于每位有0或1两个状态，输入状态至多 $2^{\lceil\log_2 n\rceil-1}<n$ 种. 因此存在 $x, y\in Z_n$，$x\neq y$，且 $\forall z\in Z_n$ 有 $(x\oplus z)_i=(y\oplus z)_i$. 根据引理，$(x-y)\otimes Z_n$ 是 Z_n 的子群，且它的每个元素的第 i 位是0，这就与 $a\in(x-y)\otimes Z_n$ 且 $(a)_i\neq 0$ 矛盾. ∎

我们称定理3.43中的 a 为无所不在的元素.

推论 1　若 Z_n 中含有一个无所不在的元素，则用 r-电路计算 Z_n 中的加法至少需要 $\lceil\log_r(2\lceil\log_2 n\rceil)\rceil$ 个时间单位.

证　由定理3.43和定理3.42可得. ∎

推论 2　若 Z_n 中不存在无所不在的元素，H 是 Z_n 的子群，H 中存在一个无所不在的元素，则用 r-电路计算 Z_n 中的加法至少需要 $\lceil\log_r(2\lceil\log_2|H|\rceil)\rceil$ 个时间单位.

证　Z_n 中加法的时间复杂性下界大于等于 H 中加法的时间复

杂性下界. ∎

下面考虑 Z_n 中是否含有无所不在的元素.

引理 1 设 $n = p^i$，p 是素数，i 是正整数，则 Z_n 中含有一个无所不在的元素.

证 Z_n 是 n 阶循环群，根据定理 3.13，对于 n 的每个正因子 p^l，$l = 1,2,\cdots i-1$，在 Z_n 中存在着唯一的 p^l 阶子群. 易见 $p, p^2, \cdots, p^{i-1}$ 是这些非平凡子群的生成元. 因此 $p^{i-1} \in Z_n$，$p^{i-1} \neq 0$，且 p^{i-1} 属于 Z_n 的每一个非平凡子群，是 Z_n 中无所不在的元素. ∎

引理 2 $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$，其中 $p_1, p_2, \cdots, p_k$ 为各不相同的素数，$i_1, i_2, \cdots, i_k$ 为正整数，则在 Z_n 中不含有无所不在的元素，且 Z_n 中含无所不在元素的最大非平凡子群的阶为 $\max\{p_1^{i_1}, p_2^{i_2}, \cdots, p_k^{i_k}\}$.

证 令 $G_j = \langle p_1^{i_1} p_2^{i_2} \cdots p_{j-1}^{i_{j-1}} p_{j+1}^{i_{j+1}} \cdots p_k^{i_k} \rangle$，$j = 1,2,\cdots,k$. 则 G_j 是 Z_n 的 $p_j^{i_j}$ 阶子群，且当 $j \neq l$ 时 $G_j \cap G_l = \{0\}$. 将 Z_n 作直积分解得 $Z_n = G_1 \times G_2 \times \cdots \times G_k$. 易见 Z_n 中不存在着无所不在的元素，否则与 $G_j \cap G_l = \{0\}$ $(j \neq l)$ 矛盾. 根据引理 1，每个 G_j 中存在着无所不在的元素，Z_n 中含无所不在元素的最大非平凡子群的阶为 $\max\{|G_1|, |G_2|, \cdots, |G_k|\} = \max\{p_1^{i_1}, p_2^{i_2}, \cdots, p_k^{i_k}\}$. ∎

定理 3.44 (1) $n = p^i$，p 为素数，i 为正整数，则用 r- 电路计算 Z_n 中加法至少需要 $\lceil \log_r \lceil 2\log_2 n \rceil) \rceil$ 个时间单位.

(2) $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ 是 n 的素因子分解式，则用 r- 电路计算 Z_n 中加法至少需要 $\lceil \log_r (2\lceil \log_2 t(n) \rceil) \rceil$ 个时间单位，其中 $t(n) = \max\{p_1^{i_1}, p_2^{i_2}, \cdots, p_k^{i_k}\}$.

证 (1) 由引理 1 和定理 3.43 的推论 1 得证.

(2) 由引理 2 和定理 3.43 的推论 2 得证. ∎

习 题 三

1. 设$G=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$,证明$G$关于矩阵乘法构成一个群.

2. 设G是群,$u\in G$,在G内定义$\circ$运算如下:$\forall a,b\in G,a\circ b=au^{-1}b$,证明$G$关于$\circ$运算构成群.

3. 设G是整数加群$\langle Z,+\rangle$,在G内定义$\circ$运算如下:$\forall a,b\in G,a\circ b=a+b-2$,证明$G$关于$\circ$运算构成群.

4. 设G是群,定义G内的$*$运算如下:$\forall a,b\in G,a*b=ba$.证明$\langle G,*\rangle$是群.

5. 证明矩阵

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}w&0\\0&w^2\end{pmatrix},\begin{pmatrix}w^2&0\\0&w\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}0&w^2\\w&0\end{pmatrix},\begin{pmatrix}0&w\\w^2&0\end{pmatrix}$$

组成的集合关于矩阵乘法构成群,其中$w^3=1,w\neq1$.

6. 设G是群,$a,b\in G$,且$(ab)^2=a^2b^2$,证明$ab=ba$.

7. 设G是群,$x,y\in G,k\in Z^+$,证明

$$(x^{-1}yx)^k=x^{-1}y^kx\text{ 的充要条件是 }y^k=y.$$

8. 证明定理3.2的(2),(4)和(5).

9. 设G是群,$a,b,c\in G$,证明

(1) $|b^{-1}ab|=|a|$;

(2) $|ab|=|ba|$;

(3) $|abc|=|bca|=|cab|$;

(4) 若$ba=a^mb^n$,则$|a^mb^{n-2}|=|ab^{-1}|,|a^{m-2}b^n|=|a^{-1}b|$.

10. 设G是偶数阶群,证明G中必存在二阶元.

11. 设G是非交换群,则G中存在着非单位元a和b,$a\neq b$且$ab=ba$.

12. G是群,$u_1,v_1,u_2,v_2\in G$且

$$u_1v_1=v_1u_1=u_2v_2=v_2u_2,$$

$$u_1^q=u_2^q=v_1^q=v_2^q=e.$$

若$(p,q)=1$，证明$u_1=u_2, v_1=v_2$.

13. 设G是$M_n(R)$上的加法群，$n\geqslant 2$，判断下列子集是否构成子群.

(1) 全体对称矩阵；

(2) 全体对角矩阵；

(3) 全体行列式$\geqslant 0$的矩阵；

(4) 全体上(下)三角矩阵.

14. 设G是群，$a\in G$且$a^2=e$，令

$$H=\{x\mid x\in G\wedge xa=ax\},$$

证明H是G的子群.

15. 找出满足以下条件的群G：

(1) 只有一个子群；

(2) 只有两个子群；

(3) 只有三个子群；

16. 设H_1,H_2是G的子群. 证明H_1H_2是G的子群的充要条件是$H_1H_2=H_2H_1$，其中

$$H_1H_2=\{h_1h_2\mid h_1\in H_1\wedge h_2\in H_2\},$$

$$H_2H_1=\{h_2h_1\mid h_2\in H_2\wedge h_1\in H_1\}.$$

17. 设H_1, H'_1, H_2, H'_2是G的子群，$H_1\subseteq H'_1$, $H_2\subseteq H'_2$，证明

$$H_1H_2\cap H'_1\cap H'_2=(H_1\cap H'_2)(H'_1\cap H_2).$$

18. (1) 找出题1中群G的所有子群并画出G的子群格.

(2) 找出题5中群G的所有子群并画出G的子群格.

19. 设$G=\langle a\rangle$是15阶循环群.

(1) 找出G的全部生成元；

(2) 找出G的全部子群并画出G的子群格.

20. 设G是群，$a,b\in G$, $|a|=p$，p为素数，若$a\notin\langle b\rangle$，证明

$$\langle a\rangle\cap\langle b\rangle=\{e\}.$$

21. 设G是rs阶循环群，$(r,s)=1$，H_1和H_2分别为G的r，s阶子群. 证明

$$G=H_1H_2.$$

22. 设$G=\langle a\rangle$是循环群，$H_1=\langle a^r\rangle$, $H_2=\langle a^s\rangle$，r,s是非负整数. 证明

$$H_1\cap H_2=\langle a^d\rangle，其中\ d=[r,s].$$

23. 证明任何无限群有无穷多个子群.

24. 在 S_5 中设

$$\sigma=\begin{pmatrix}1&2&3&4&5\\5&1&4&3&2\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}.$$

计算：

(1) $\sigma\tau,\tau\sigma,\sigma^{-1},\tau^{-1}$；

(2) 将 σ 和 τ 表成不相交的轮换之积和对换之积.

25. 证明 S_n 可由 $\{(12),(13),\cdots,(1n)\}$ 生成，也可由 $\{(12),(23),\cdots,(n-1\ \ n)\}$ 生成.

26. 在 S_5 中设

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}.$$

(1) 求解群方程 $\sigma x=\tau$ 和 $y\sigma=\tau$；

(2) 求 $|\sigma|$ 和 $|\tau|$.

27. 在 S_4 中取子群 $H=\langle(1234)\rangle$，写出 H 在 S_4 中的全部右陪集.

28. 设 $G=\left\{\begin{pmatrix}r&s\\0&1\end{pmatrix}\middle|\, r,s\in Q,r\neq 0\right\}$，$G$ 关于矩阵乘法构成一个群. $H=\left\{\begin{pmatrix}1&t\\0&1\end{pmatrix}\middle|\, t\in Q\right\}$ 是 G 的子群. 求 H 在 G 中的全部左陪集.

29. 证明定理 3.25.

30. 设 H_1,H_2 分别是 G 的 r,s 阶子群. 若 $(r,s)=1$，证明 $H_1\cap H_2=\{e\}$.

31. 设 p 是素数，m 是正整数. 证明 p^m 阶群必有 p 阶子群.

32. 设 G 是有限群，K 是 G 的子群，H 是 K 的子群. 证明

$$[G:H]=[G:K][K:H].$$

33. 设 A,B 是群 G 的有限子群，则

(1) $|AB|=\dfrac{|A||B|}{|A\cap B|}$；

(2) 若 $(|A|,|B|)=1$，则 $|AB|=|A||B|$.

34. 证明 S_n 中同一共轭类的元素都具有相同的轮换指数.

35. 求题 26 中的 σ 和 τ 的轮换指数.

36. 证明定理 3.29.

37. 若把群看作具有一个二元运算、一个一元运算和一个零元运算的代数系统，证明共轭关系是群上的同余关系.

38. 设 G 是 4 阶群，

(1) 若 G 为循环群 $\langle a\rangle$，求 G 的所有共轭类；

(2) 若 G 为 Klein 四元群，求 G 的所有共轭类.

39. 设 G 为群，$a \in G$，$N(a)$ 是 a 的正规化子. 证明 $\forall x \in G$，$x^{-1}ax$ 的正规化子 $N(x^{-1}ax) = x^{-1}N(a)x$.

40. 设 G 为有限群，$a \in G$，若 $|\bar{a}| = k$，$|\overline{a^r}| = k'$，证明 k' 整除 k.

41. 设 G 为 n 阶群，$a \in G$，若 $|\bar{a}| = k$，C 是 G 的中心，且 $|C| = c$. 证明 k 整除 $\frac{n}{c}$.

42. 证明循环群的任何子群都是正规子群.

43. 对于题 28 中的 G 和 H 证明 H 是 G 的正规子群.

44. 设 N, K 是 G 的子群，$H = \langle N \cup K \rangle$ 是由 $N \cup K$ 生成的子群，若 N 是 H 的正规子群，则 $H = KN$.

45. 设 N 是 G 的正规子群，且 $|N| = 2$. 证明 $N \subseteq C$，其中 C 是 G 的中心.

46. 设 G 是全体 $n \times n$ 实可逆矩阵关于矩阵乘法构成的群，H 是 G 中全体行列式大于 0 的矩阵集合.

(1) 证明 $H \trianglelefteq G$；

(2) 计算 $[G : H]$.

47. 设

$$G_1 = \{A \mid A \in M_n(Q) \land |A| \neq 0\}.$$

其中 $M_n(Q)$ 是有理数域上的 n 阶矩阵集合 $(n \geqslant 2)$. G_1 关于矩阵乘法构成群. φ 是 G_1 到 $G_2 = \langle R^*, \cdot \rangle$ 的映射，$\varphi(A) = |A|$，$\forall A \in M_n(Q)$，其中 $\cdot$ 为普通乘法.

(1) 证明 φ 是 G_1 到 G_2 的同态映射；

(2) 求出 $\varphi(G_1)$ 和 $\ker\varphi$.

48. 证明除零同态以外，不存在 $\langle Q, + \rangle$ 到 $\langle Z, + \rangle$ 的同态映射.

49. 设 φ_1 是群 G_1 到 G_2 的同构，φ_2 是群 G_2 到 G_3 的同构，证明 $\varphi_2 \circ \varphi_1$ 是群 G_1 到 G_3 的同构.

50. 设 φ 是群 G_1 到 G_2 的同构，证明 φ^{-1} 是 G_2 到 G_1 的同构.

51. 设 φ 是群 G_1 到 G_2 的同态映射，证明

(1) 若 H 是 G_2 的子群，则 $\varphi^{-1}(H)$ 是 G_1 的子群；

(2) 若 H 是 G_2 的正规子群，则 $\varphi^{-1}(H)$ 是 G_1 的正规子群.

52. 设 $G_1 = \langle a \rangle$，$G_2 = \langle b \rangle$ 分别为 m, n 阶循环群. $\varphi: G_1 \to G_2$，$\varphi(a^t) = b^{kt}$，$t = 0, 1, \cdots, m-1$. 证明 φ 为 G_1 到 G_2 的同态映射当且仅当 $n \mid mk$.

53. 设φ是群G_1到G_2的满同态映射,H是G_1的子群.若$|H|$与$|G_2|$互素,证明$H\subseteq\ker\varphi$.

54. 设H是G的子群,N是G的正规子群.如果$|H|$与$[G:N]$互素,证明H是N的子群.

55. 设φ是群G_1到G_2的满同态,N是G_1的正规子群,且$\ker\varphi\subseteq N$.证明

$$G_1/N\cong G_2/\varphi(N).$$

56. 设H,K是群G的正规子群,证明

$$G/HK\cong(G/H)/(HK/H).$$

57. 证明阶为p^2的群必是交换群,其中p是素数.

58. 设G是pq阶交换群,p,q为不相等的素数.对于G的任一子群H,证明G/H是循环群.

59. 证明在同构的意义上Klein四元群是S_4的正规子群.

60. 设φ是群G的满自同态,若G只有有限个子群,证明φ是G的自同构.

61. 在群G中定义φ: $x\mapsto x^{-1}$, $\forall x\in G$.证明φ是G的自同构的充分必要条件是G为交换群.

62. 设$G=\langle a\rangle$是n阶循环群,t是正整数.定义

$$\varphi_t: a^i\mapsto(a^t)^i,\ i=0,1,\cdots,n-1.$$

证明

(1) φ_t是G的自同态;

(2) φ_t是G的自同构当且仅当$(n,t)=1$.

63. 设G是群,C是G的中心,证明$G/C\cong\mathrm{Inn}G$.

64. 证明在同构的意义上只有两个10阶群.

65. 对什么样的群G,$\mathrm{Inn}G$只含一个恒等映射?

66. 设G_1,G_2是群,证明$G_2\times G_1\cong G_2\times G_1$.

67. 设H_1是G_1的子群,H_2是G_2的子群,证明$H_1\times H_2$是$G_1\times G_2$的子群.

68. 设H和K是G的正规子群,且$H\cap K=\{e\}$.证明G与$G/H\times G/K$的一个子群同构.

69. 找出$G_1\times G_2$的两个商群$G_1\times G_2\big/N_1$,$G_1\times G_2\big/N_2$,使得

$$G_1\cong G_1\times G_2\big/N_1,\ G_2\cong G_1\times G_2\big/N_2.$$

第四章　环与域

环和域是具有两个二元运算的代数系统. 本章先给出环的定义和性质，然后讨论子环、理想、商环以及域.

§ 4.1　环的定义和性质

先给出环的定义.

定义 4.1　设 $\langle R, +, \cdot\rangle$ 是具有两个二元运算的代数系统，如果满足以下条件：

(1) $\langle R, +\rangle$ 构成 Abel 群，

(2) $\langle R, \cdot\rangle$ 构成半群，

(3) R 中的 $\cdot$ 对 $+$ 适合分配律，

则称 $\langle R, +, \cdot\rangle$ 是**环**，并称 $+$ 和 $\cdot$ 分别为环中的加法和乘法.

【例 4.1】

(1) 整数集 Z，有理数集 Q，实数集 R 和复数集 C 关于普通数的加法和乘法构成环，分别称作**整数环**，**有理数环**，**实数环**和**复数环**.

(2) 设 $n \geqslant 2$，$M_n(R)$ 为 n 阶实矩阵的集合，则 $M_n(R)$ 关于矩阵加法和乘法构成环，称为 **n 阶实矩阵环**.

(3) $\langle Z_n, \oplus, \otimes\rangle$ 构成一个环，其中 $Z_n = \{0,1,\cdots,n-1\}$，$\forall x, y \in Z_n$，$x \oplus y = (x+y)\bmod n$，$x \otimes y = (xy)\bmod n$，称这个环为**模 n 整数环**.

(4) $\langle P(B), \oplus, \cap\rangle$ 构成一个环，其中 $\oplus$ 为集合的对称差运算.

(5) 设 $\langle G, \circ\rangle$ 是 Abel 群. 在 G 上定义 $*$ 运算，$\forall x, y \in G$，$x * y = e$，则 $\langle G, \circ, *\rangle$ 构成一个环，称为**零环**.

为了叙述上的方便，通常将环中加法的单位元记作 0，而将环中元素 x 关于加法的逆元称作 x 的**负元**，记作 $-x$. 如果环中乘法有单位元，就把这个单位元记作 1，而将 x 关于乘法的逆元(若存在的话)

称为 x 的逆元，记作 x^{-1}. 类似地，我们可以用 $x-y$ 表示 $x+(-y)$，nx 表示 x 的加法 n 次幂，即 $nx=\underbrace{x+x+\cdots+x}_{n个}$. 而用 x^n 表示 x 的乘法 n 次幂，即 $x^n=\underbrace{xx\cdots x}_{n个}$.

下面讨论环的运算性质. 由环的定义可知，环中加法适合交换律、结合律，有单位元 0，每个元素都有负元，环中乘法适合结合律，乘法对加法适合分配律. 除此之外，环还有一些其它的运算性质.

定理 4.1 设 R 是环，则

(1) $\forall a\in R,\ a0=0a=0$；

(2) $\forall a,b\in R,\ (-a)b=a(-b)=-(ab)$；

(3) $\forall a,b\in R,\ (-a)(-b)=ab$；

(4) $\forall a,b,c\in R$ 有

$$a(b-c)=ab-ac,$$
$$(b-c)a=ba-ca;$$

(5) $\forall a_1,a_2,\cdots,a_n,\ b_1,b_2,\cdots,b_m\in R$ 有

$$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j;$$

(6) $\forall a,b\in R,\ n\in Z,(na)b=a(nb)=n(ab)$.

证 (1) $a0=a(0+0)=a0+a0$.

由加法消去律得 $a0=0$. 同理可证 $0a=0$.

(2) $(-a)b+ab=(-a+a)b=0b=0$,

$$ab+(-a)b=(a+(-a))b=0\,b=0.$$

这就推出 $(-a)b$ 是 ab 的负元，根据负元的唯一性得 $(-a)b=-(ab)$. 同理可证 $a(-b)=-(ab)$.

(3) $(-a)(-b)=-(a(-b))=-(-(ab))=ab$.

(4) $a(b-c)=a(b+(-c))=ab+a(-c)$

$$=ab+(-(ac))=ab-ac.$$

同理有 $(b-c)a=ba-ca$.

(5) 先证对任意 $i=1,2,\cdots,n$ 有

$$a_i\left(\sum_{j=1}^{m}b_j\right)=\sum_{j=1}^{m}a_ib_j.$$

对 m 进行归纳.

$m=2$，由环中乘法对加法的分配律有

$$a_i(b_1+b_2)=a_ib_1+a_ib_2.$$

假设 $m=k$ 时等式成立，当 $m=k+1$ 时有

$$\begin{aligned}a_i\left(\sum_{j=1}^{k+1}b_j\right)&=a_i\left(\sum_{j=1}^{k}b_j+b_{k+1}\right)=a_i\left(\sum_{j=1}^{k}b_j\right)+a_ib_{k+1}\\&=\sum_{j=1}^{k}a_ib_j+a_ib_{k+1}=\sum_{j=1}^{k+1}a_ib_j.\end{aligned}$$

同理可证对任意环中元素 b_j 有

$$\left(\sum_{i=1}^{n}a_i\right)b_j=\sum_{i=1}^{n}a_ib_j.$$

因此，$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}a_i\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j.$

(6) 先证 $(na)b=n(ab)$. 考虑 $n>0$，对 n 归纳.

$n=1$ 时，左边与右边都是 ab.

假设 $n=k$ 时等式成立，则有

$$\begin{aligned}((k+1)a)b&=(ka+a)b=(ka)b+ab=k(ab)+ab\\&=(k+1)(ab),\end{aligned}$$

由归纳法知对一切 $n\in Z^+$ 等式都成立.

当 $n=0$ 时，等式两边都是 0，等式也成立.

当 $n<0$ 时，令 $n=-m$，$m\in Z^+$，则有

$$\begin{aligned}(na)b&=(-ma)b=(m(-a))b=m((-a)b)=m(-(ab))\\&=-m(ab)=n(ab).\end{aligned}$$

同理可证 $a(nb)=n(ab)$. ∎

定理 4.1 说明环中加法的单位元 0 恰为环中乘法的零元. 在环

中作公式展开时可以使用定理中的等式.

【例 4.2】 设 R 是环,$a,b \in R$,计算 $(a-b)^2$ 和 $(a+b)^3$.

解 $(a-b)^2 = (a-b)(a-b) = a^2 - ba - ab + b^2$,

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)(a+b)\\ &= (a^2+ba+ab+b^2)(a+b)\\ &= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3.\end{aligned}$$

【例 4.3】 在模 3 的整数环 Z_3 中解方程组

$$\begin{cases} x+2z=1, & ①\\ y+2z=2, & ②\\ 2x+y=1. & ③\end{cases}$$

解 ① − ② 得 $x-y=2$. ④

③ + ④ 得 $3x=0$.

② − ① 得 $y-x=1$.

若 $x=0$,则 $y=1$,从而推得 $z=2$. 若 $x=1,y=2$,从而推得 $z=0$. 若 $x=2,y=0$,从而推得 $z=1$. 原方程组有三组解:

$$\begin{cases} x_1=0,\\ y_1=1,\\ z_1=2;\end{cases}\quad \begin{cases} x_2=1,\\ y_2=2,\\ z_2=0;\end{cases}\quad \begin{cases} x_3=2,\\ y_3=0,\\ z_3=1.\end{cases}$$

设 $\langle R,+,\cdot\rangle$ 是环,如果环中乘法满足除结合律以外的其它算律,就得到一些特殊的环.

定义 4.2 设 a,b 是环 R 中的两个非零元素,如果 $ab=0$,则称 a 是 R 中的一个**左零因子**,b 是 R 中的一个**右零因子**;若一个元素既是左零因子又是右零因子,则称它是一个**零因子**.

例如模 6 的整数环中,$2 \otimes 3 = 0$,2 是左零因子,3 是右零因子,又由于 $\otimes$ 是可交换的,所以 2 也是右零因子,3 也是左零因子. 2 和 3 都是零因子.

定义 4.3 设 R 是一个环,对于任意的 $a,b \in R$,若 $ab=0$,则有 $a=0$ 或 $b=0$,就称 R 是一个**无零因子环**.

不难看出，无零因子环就是不含有左和右零因子的环.

例如数环，包括整数环、有理数环、实数环、复数环等，都是无零因子环.

【例 4.4】 证明 Z_p 为无零因子环当且仅当 p 为素数.

证 必要性.假设 p 不是素数，必存在小于 p 大于 1 的正整数 s，t 使得 $p = st$. 易见 $(st)\bmod p = 0$，s 和 t 是 Z_p 中的零因子，与 Z_p 是无零因子环矛盾.

充分性.任取 $a, b \in Z_p$，若 $ab = 0$，不妨设 $a \neq 0$，我们证明必有 $b = 0$.

由 $ab = 0$ 可知 $p \mid ab$. 由 $a, b \in \{0, 1, \cdots, p-1\}$ 知 $p \nmid a$. 而 p 又是素数，所以 $p \mid b$，从而 $b = 0$. ▮

定理 4.2 设 R 是环. R 是无零因子环的充分必要条件是在 R 中乘法适合消去律，即对于任意 $a, b, c \in R$，$a \neq 0$，若有 $ab = ac$（或 $ba = ca$），则有 $b = c$.

证 充分性.设 R 中乘法满足消去律.任取 $a, b \in R$，且 $ab = 0$，$a \neq 0$，则有 $ab = 0 = a0$. 由消去律得 $b = 0$，R 是无零因子环.

必要性.任取 $a, b, c \in R$，$ab = ac$ 且 $a \neq 0$，则有 $ab - ac = 0$. 由定理 4.1 得 $a(b-c) = 0$. 因为 R 中没有零因子，所以 $b - c = 0$，即 $b = c$. 同理可证 $ba = ca$ 且 $a \neq 0 \Rightarrow b = c$. ▮

由以上定理可知无零因子环是和乘法消去律联系在一起的. 如果环中乘法再满足其它条件就构成整环.

定义 4.4 设 R 是一个环，

(1) 若 R 中乘法适合交换律，则称 R 是**交换环**；

(2) 若 R 中乘法含有单位元，则称 R 是**含幺环**；

(3) 若 R 是交换的含幺的无零因子环，则称 R 是**整环**.

例如有理数环 Q，实数环 R，复数环 C 都是整环. 整数环 Z 也是整环，但模 n 整数环 Z_n 只有当 n 是素数时才是整环. 当 $n \geq 2$ 时，n 阶实矩阵环 $M_n(R)$ 不是整环，因为矩阵乘法不是可交换的.

定义 4.5 设 R 是一个环，

(1) 若 R 中至少含有两个元素，令 $R^* = R - \{0\}$，且 $\langle R^*, \cdot \rangle$ 构成群，则称 R 是一个**除环**；

(2) 若 R 是一个交换的除环，则称 R 是**域**.

【例 4.5】 下述集合关于所指出的运算是否构成环？是否构成整环？是否构成除环？是否构成域？

(1) $\{a + b\sqrt{2} \mid a, b \in Z\}$ 关于数的加法和乘法；

(2) $\{a + b\sqrt{2} \mid a, b \in Q\}$ 关于数的加法和乘法；

(3) $\{a + b\sqrt[3]{2} \mid a, b \in Z\}$ 关于数的加法和乘法；

(4) $\{a + bi \mid a, b \in Z, i^2 = -1\}$ 关于复数的加法和乘法；

(5) 设 $n \geqslant 2$，n 阶实矩阵集合 $M_n(R)$ 关于矩阵的加法和乘法；

(6) 集合 $\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in Z\right\}$ 关于矩阵加法和乘法；

(7) x 的实系数多项式集合关于多项式的加法和乘法；

(8) 实数集 R 关于加法 $+$ 和乘法 $*$，其中 $+$ 是普通加法，$\forall a, b \in R, a * b = |a| b$.

解 (1) 是整环，但不是除环和域.

(2) 是整环，除环和域.

(3) 不是环，关于乘法运算不封闭.

(4) 是整环，不是除环和域.

(5) 是环，但不是整环，除环和域.

(6) 是环，但不是整环、除环和域.

(7) 是整环，不是除环和域.

(8) 不是环，因为 $*$ 对 $+$ 不适合分配律.

如果一个域是有限的，称为**有限域**. 下面考虑有限域中的一些性质.

定义 4.6 设 F 是有限域，称 1 在 $\langle F, + \rangle$ 中的阶为 F 的**特征**.

例如 Z_3 是有限域，Z_3 的特征是 3.

定理 4.3 设 F 为有限域，则 F 的特征是素数.

证 假设 1 在 $\langle F, +\rangle$ 中的阶为 $n, n \in Z^+$. 若 n 不是素数，则存在 $p, q \in Z^+$，使得 $n = pq$，且 $p, q \geqslant 2$. 令 $t \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{t个}$，

则

$$(p \cdot 1)(q \cdot 1) = pq \cdot 1 = n \cdot 1 = 0.$$

因为域中无零因子，必有 $p \cdot 1 = 0$ 或 $q \cdot 1 = 0$，与 1 在 $\langle F, +\rangle$ 中的阶是 n 矛盾. ∎

定理 4.4 设 F 为有限域，则存在素数 p，使得 $|F| = p^n$，其中 $n \in Z^+$.

证 由定理 4.3，F 的特征为 p，令

$$A = \{0, 1, \cdots, p-1\}$$

是由 1 生成的加法子群，任取 $x_1 \in F^*$，令

$$Ax_1 = \{0, x_1, \cdots, (p-1)x_1\}.$$

若 $Ax_1 = F$，则 $|F| = p$. 否则存在 $x_2 \in F - Ax_1$，令

$$Ax_1 + Ax_2 = \{a_1x_1 + a_2x_2 \mid a_1, a_2 \in A\},$$

则 $|Ax_1 + Ax_2| = p^2$. 因为 $\forall i_1, i_2, j_1, j_2 \in A$，如果 $i_1 \neq j_1$ 或 $i_2 \neq j_2$，则 $i_1x_1 + i_2x_2 \neq j_1x_1 + j_2x_2$. 若不然，必有 $(i_1 - j_1)x_1 + (i_2 - j_2)x_2 = 0$. 这说明存在 $a_1, a_2 \in A$ 使得 $a_1x_1 = a_2x_2, a_1, a_2 \neq 0$. 因此可得 $x_2 = a_2^{-1}a_1x_1 \in Ax_1$，矛盾.

若 $F = Ax_1 + Ax_2$，则 $|F| = p^2$. 否则存在 $x_3 \in F - (Ax_1 + Ax_2)$，令

$$Ax_1 + Ax_2 + Ax_3 = \{a_1x_1 + a_2x_2 + a_3x_3 \mid a_1, a_2, a_3 \in A\},$$

则 $|Ax_1 + Ax_2 + Ax_3| = p^3$. 若不然必存在 $i_1, i_2, i_3, j_1, j_2, j_3 \in A$，使得

$$(i_1 - j_1)x_1 + (i_2 - j_2)x_2 + (i_3 - j_3)x_3 = 0.$$

如果 $(i_1 - j_1)x_1 + (i_2 - j_2)x_2 = 0$，与 $x_2 \notin Ax_1$ 矛盾，所以 $i_3 - j_3 \neq 0$，x_3 可以表为 $a_1x_1 + a_2x_2$ 的形式，这说明 $x_3 \in Ax_1 + Ax_2$，矛盾.

根据归纳证明不难得到

$$|F| = |Ax_1 + Ax_2 + \cdots + Ax_n| = p^n,$$

其中 $n \in Z^+$.

∎

由有限域 F 可以得到 F 上的多项式环,有关的内容将在后面加以介绍.

§ 4.2 子环、理想、商环和环同态

定义 4.7 设 $\langle R, +, \cdot\rangle$ 是环,S 是 R 的非空子集,若 S 关于环 R 的运算 $+$ 和 $\cdot$ 构成环,则称 $\langle S, +, \cdot\rangle$ 是 R 的**子环**,$\langle R, +, \cdot\rangle$ 是 $\langle S, +, \cdot\rangle$ 的**扩环**.

例如 $\langle Z, +, \cdot\rangle$ 是 $\langle Q, +, \cdot\rangle$ 和 $\langle R, +, \cdot\rangle$ 的子环,其中 R 为实数集. $\langle nZ, +, \cdot\rangle$ 是 $\langle Z, +, \cdot\rangle$ 的子环,而 $\langle R, +, \cdot\rangle$ 是 $\langle Z, +, \cdot\rangle$ 和 $\langle Q, +, \cdot\rangle$ 的扩环.

由子环定义可知环 R 的子环就是 R 的子代数. 根据子群和子半群的判定定理可直接得到子环的判定定理.

定理 4.5 环 R 的非空子集 S 是 R 的一个子环的充分必要条件是:对任意 $a,b \in S$ 有

(1) $a - b \in S$;

(2) $ab \in S$.

【例 4.6】 设 R 是环,令

$$C = \{x | x \in R \land \forall a \in R(ax = xa)\}.$$

证明 C 是 R 的子环,叫做 R 的**中心**.

证 易见 $0 \in C$,C 非空. 任取 $x,y \in C$,对任意的 $a \in R$,

$$(x - y)a = xa - ya = ax - ay = a(x - y).$$

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

这就证明了 $x - y \in C$ 和 $xy \in C$. 由定理 4.5 知 C 是 R 的子环. ∎

【例 4.7】 设 R 是环,A 是 R 的子环族,证明 $\bigcap A$ 是 R 的子环,其中

$$\bigcap A = \{x | \forall z(z \in A \to x \in z)\}.$$

证 易见 0 属于 R 的每个子环，所以 $0 \in \bigcap A$，$\bigcap A$ 非空.

任取 $a,b \in \bigcap A$，则对每个 $S \in A$，有 $a,b \in S$. 因为 S 是 R 的子环，所以 $a-b$ 和 ab 属于 S，从而得到 $a-b \in \bigcap A$ 和 $ab \in \bigcap A$. 根据定理 4.5 可知 $\bigcap A$ 是 R 的子环. ∎

对于任意的环 R，R 的子环都是存在的. 特别地，R 和 $\{0\}$ 都是 R 的子环，称为**平凡子环**.

类似地可以定义子整环，子除环和子域.

定义 4.8 设 R 是环，S 是 R 的非空子集，

(1) 如果 R 是整环，S 对 R 的运算仍构成整环，则称 S 是 R 的**子整环**；

(2) 如果 R 是除环，S 对 R 的运算仍构成除环，则称 S 是 R 的**子除环**；

(3) 如果 R 是域，S 对 R 的运算仍构成域，则称 S 是 R 的**子域**.

【例 4.8】 设 S 是域 F 的子环且 $S \neq \{0\}$. 证明 S 是 F 的子域当且仅当对任意的 $x \in S$，只要 $x \neq 0$，均有 $x^{-1} \in S$.

证 令 $S^* = S - \{0\}$.

必要性. 若 S 是 F 的子域，则 $\langle S^*, \cdot \rangle$ 是群，对任意 $x \in S^*$ 显然有 $x^{-1} \in S^*$，即 $x^{-1} \in S$.

充分性. 任取 $x,y \in S^*$，则 $x,y \in S$. 因为 S 是子环，必有 $xy \in S$，$xy \neq 0$，否则由 $xy \in F$ 得 $x=0$ 或 $y=0$，从而证明了 $xy \in S^*$. 任取 $x \in S^*$，由已知有 $x^{-1} \in S$ 且 $x^{-1} \neq 0$，所以 $x^{-1} \in S^*$. 于是 $\langle S^*, \cdot \rangle$ 构成群，是 $\langle F^*, \cdot \rangle$ 的子群. 这就证明 S 关于 F 中运算构成域，是 F 的子域. ∎

【例 4.9】 证明有理数域无真子域.

证 设 S 是 Q 的任一子域，则 $1 \in S$，从而任意正整数 $p = \underbrace{1+1+\cdots+1}_{p\text{个}} \in S$，且 $-p \in S$. 设 q 为任意正整数，$q \neq 0$，则 $\dfrac{1}{q} \in$

S.根据乘法封闭性有 $\pm \frac{p}{q} \in S$,这就推出 $Q \subseteq S$,因此 $S = Q$.

∎

回顾上一章可知正规子群是一类很重要的子群,通过它可以得到群的商群,在环中和正规子群相对应的概念是理想,通过理想可以得到商环.

定义 4.9 设 $\langle R, +, \cdot \rangle$ 是环,D 是 R 的非空子集,若

(1) $\langle D, + \rangle$ 构成 Abel 群,

(2) $\forall r \in R$ 有 $rD \subseteq D$ 和 $Dr \subseteq D$,

则称 D 为环 R 的**理想**.

【例 4.10】 设 $R = \langle Z, +, \cdot \rangle$ 是整数环,则 nZ 是 R 的理想,其中 n 为自然数. 易见 $\langle nZ, + \rangle$ 是 Abel 群. 任取 $k \in Z$,有

$$knz \in nZ \quad 和 \quad nzk \in nZ.$$

即 $knZ \subseteq nZ$ 和 $nZk \subseteq nZ$,所以 nZ 为 R 的理想.

由定义 4.9 不难证明环 R 的理想 D 一定是 R 的子环,但环 R 的任一子环不一定是 R 的理想. 设 D 是 R 的理想,$\forall x, y \in D$,则 $x - y \in D$,且 $xy \in xD \subseteq D$. 所以 D 是 R 的子环. 但反之不一定为真. 例如 $\langle Z, +, \cdot \rangle$ 是 $\langle R, +, \cdot \rangle$ 的子环,其中 Z 和 R 分别为整数集和实数集,但 $\langle Z, +, \cdot \rangle$ 不是 $\langle R, +, \cdot \rangle$ 的理想.

对于任何环 R 都有两个**平凡理想**,就是 R 的两个平凡子环 R 和 $\{0\}$,除此之外的理想习惯上叫做 R 的**真理想**(注意这里的"真"与真子代数的"真"有点区别. $\{0\}$ 是 R 的真子集,也是 R 的理想,但不叫做 R 的真理想).

【例 4.11】 设 R 是交换环,且 $1 \neq 0$. 则 R 为域当且仅当 R 只含平凡理想.

证 必要性. 设 D 是 R 的理想且 $D \neq \{0\}$,则存在 $x \in D, x \neq 0$. 由于 R 是域,必有 $x^{-1} \in R$,满足 $xx^{-1} = 1$,因此 $1 \in D$. 任取 $r \in R$,有 $r = r \cdot 1 \in D$,所以 $R \subseteq D$,从而有 $D = R$.

充分性. 设 R 只含平凡理想，任取 $x \in R, x \neq 0$，则易证

$$D = Rx = \{rx \mid r \in R\}$$

是 R 的理想，从而有 $Rx = R$. 这就证明了存在 $y \in R$，使得 $yx = 1$. 因为乘法是可交换的，y 是 x 的逆元. $\langle R^*, \cdot \rangle$ 构成 Abel 群，因此 R 是域. ∎

由环和理想可以构造商环.

定义 4.10 设 D 是环 R 的理想. 对于任意的 $x \in R$，x 关于加法的陪集记作 $\bar{x}$，即 $\bar{x} = D + x = \{d + x \mid d \in D\}$. 令 $R/D = \{\bar{x} \mid x \in R\}$ 是 D 的全体加法陪集的集合，在 R/D 上定义二元运算

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{xy},$$

则 $\langle R/D, +, \cdot \rangle$ 构成一个环，称为 R 关于 D 的**商环**.

为了保证以上定义的正确性，我们必须验证商环中的两个运算是良定义的.

因为 $\langle R, + \rangle$ 是 Abel 群，$\langle D, + \rangle$ 是正规子群，所以 R/D 关于商环中的加法构成商群. 显然商环中的加法是良定义的、可结合的，也是可交换的.

任取 $\bar{x}, \bar{y} \in R/D$，$\overline{x'}, \overline{y'} \in R/D$. 假设 $\overline{x'} = \bar{x}$，$\overline{y'} = \bar{y}$，则有 $d_1, d_2 \in D$，使得

$$x' = d_1 + x, \ y' = d_2 + y.$$

因此有

$$\overline{x'} \cdot \overline{y'} = \overline{(d_1 + x)(d_2 + y)} = \overline{d_1 d_2 + d_1 y + x d_2 + xy}.$$

由于 D 是理想，$d_1 d_2 + d_1 y + x d_2 \in D$，从而得到

$$\overline{x'} \cdot \overline{y'} = \overline{d + xy} = \overline{xy} = \bar{x} \cdot \bar{y}.$$

这就验证了商环中的乘法也是良定义的. 下面证明乘法是可结合的.

任取 $\bar{x}, \bar{y}, \bar{z} \in R/D$，有

$$(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \overline{xy} \cdot \bar{z} = \overline{(xy)z} = \overline{x(yz)} = \bar{x} \cdot \overline{yz} = \bar{x} \cdot (\bar{y} \cdot \bar{z}),$$

于是 $\langle R/D, \cdot \rangle$ 构成半群.

最后证明乘法对加法适合分配律，任取 $\bar{x}, \bar{y}, \bar{z} \in R/D$，有

$$\bar{x}\cdot(\bar{y}+\bar{z})=\bar{x}\cdot\overline{y+z}=\overline{x(y+z)}$$
$$=\overline{xy+xz}=\overline{xy}+\overline{xz}=\bar{x}\cdot\bar{y}+\bar{x}\cdot\bar{z}.$$

同理有

$$(\bar{y}+\bar{z})\cdot\bar{x}=\bar{y}\cdot\bar{x}+\bar{z}\cdot\bar{x}.$$

综上所述,$\langle R/D, +, \cdot\rangle$ 构成一个环.

商环 R/D 就是环 R 的商代数,对于任意的 $x,y,u,v\in R$,如果 $\bar{x}=\bar{y},\bar{u}=\bar{v}$,则有 $\bar{x}+\bar{u}=\bar{y}+\bar{v},\bar{x}\cdot\bar{u}=\bar{y}\cdot\bar{v}$.这就说明当 $x\sim y$, $u\sim v$ 时有 $x+u\sim y+v$ 和 $xu\sim yv$,即由加法陪集作为等价类所确定的等价关系是环 R 中的同余关系,所以商环 R/D 是环 R 的商代数.

【例 4.12】 设环 $R=\langle Z, +, \cdot\rangle$ 是整数环,$4Z=\{4k|k\in Z\}$ 是 R 的理想,商环 $\langle Z/4Z, \oplus, \otimes\rangle$ 称为**模 4 的剩余类环**,其中

$$Z/4Z=\{4Z,4Z+1,4Z+2,4Z+3\}=\{\bar{0},\bar{1},\bar{2},\bar{3}\},$$

且 $\bar{i}\oplus\bar{j}=\overline{i+j}$, $\bar{i}\otimes\bar{j}=\overline{ij}$, 不难看出,模 4 的剩余类环与模 4 整数环 $\langle Z_4, \oplus, \otimes\rangle$ 是同构的.

下面考虑环的同态.根据一般代数系统的同态概念,环同态定义如下:

定义 4.11 设 $\langle R_1, +, \cdot\rangle$,$\langle R_2, +, \cdot\rangle$ 是环,φ: $R_1\rightarrow R_2$.若对任意的 $x,y\in R_1$ 有

$$\varphi(x+y)=\varphi(x)+\varphi(y),$$
$$\varphi(x\cdot y)=\varphi(x)\cdot\varphi(y),$$

则称 φ 是环 R_1 到 R_2 的同态映射,简称同态.若 φ 为满射,则称 φ 是满同态;若 φ 为单射,则称 φ 为单同态;若 φ 为双射,则称 φ 为同构.

例如环 $R_1=\langle Z, +, \cdot\rangle$ 为整数环,$R_2=\langle Z_n, \oplus, \otimes\rangle$ 为模 n 整数环.则 φ: $Z\rightarrow Z_n$, $\varphi(x)=(x)\mathrm{mod}n$, $\forall x\in Z$,是 R_1 到 R_2 的满同态.

第一章中关于一般代数系统同态的定理对环都适用.下面考虑环同态的一些特殊性质.

定义 4.12 设 φ 是环 R_1 到 R_2 的同态，令

$$I = \{x | x \in R_1 \land \varphi(x) = 0\},$$

称 I 为**环同态的核**，记作 $\ker\varphi$.

定理 4.6 设 $\varphi: R_1 \to R_2$ 是环同态，则 $\ker\varphi$ 是环 R_1 的理想.

证 φ 为环 R_1 到 R_2 的同态，φ 将 Abel 群 $\langle R_1, +\rangle$ 映到 Abel 群 $\langle R_2, +\rangle$，$\ker\varphi$ 是群同态的核，由定理 3.36 知 $\ker\varphi$ 是 $\langle R_1, +\rangle$ 的正规子群.

任取 $x \in \ker\varphi, r \in R_1$，则

$$\varphi(xr) = \varphi(x)\varphi(r) = 0\varphi(r) = 0,$$

所以 $xr \in \ker\varphi$. 同理 $rx \in \ker\varphi$. 从而 $\ker\varphi$ 是环 R_1 的理想. ∎

定理 4.7 设 $\varphi: R_1 \to R_2$ 是环同态，那么

(1) 若 S 是 R_1 的子环，则 $\varphi(S)$ 是 R_2 的子环；

(2) 若 T 是 R_2 的子环，则 $\varphi^{-1}(T)$ 是 R_1 的子环；

(3) 若 D 是 R_1 的理想，则 $\varphi(D)$ 是 $\varphi(R_1)$ 的理想；

(4) 若 I 是 R_2 的理想，则 $\varphi^{-1}(I)$ 是 R_1 的理想.

证 (1) $\varphi(S)$ 非空. 任取 $a,b \in \varphi(S)$，存在 $x,y \in S$，使得 $\varphi(x) = a, \varphi(y) = b$，那么有

$$a - b = \varphi(x) - \varphi(y) = \varphi(x - y).$$

由于 $x - y \in S$，所以 $a - b \in \varphi(S)$，同时也有

$$ab = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi(S).$$

由定理 4.5，$\varphi(S)$ 是 R_2 的子环.

(2) 易见 $\varphi^{-1}(T) \neq \varnothing$. 任取 $x,y \in \varphi^{-1}(T)$，存在 $a,b \in T$ 使得 $\varphi(x) = a, \varphi(y) = b$，那么

$$\varphi(x - y) = \varphi(x) - \varphi(y) = a - b \in T,$$

则 $x - y \in \varphi^{-1}(T)$. 又

$$\varphi(xy) = \varphi(x)\varphi(y) = ab \in T,$$

即 $xy \in \varphi^{-1}(T)$. 这就证明 $\varphi^{-1}(T)$ 是 R_1 的子环.

(3) D 是 $\langle R_1, +, \cdot\rangle$ 的理想，所以 $\langle D, +\rangle$ 是 $\langle R_1, +\rangle$ 的子群. 由

定理 3.35 知$\langle \varphi(D), + \rangle$ 是$\langle \varphi(R_1), + \rangle$ 的子群，且是 Abel 群.

任取 $x \in \varphi(D)$，$r \in \varphi(R_1)$，存在 $a \in D$，$b \in R_1$，使得 $\varphi(a) = x$，$\varphi(b) = r$，且

$$xr = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(D).$$

同理 $rx \in \varphi(D)$，这就证明 $\varphi(D)$ 是 $\varphi(R_1)$ 的理想.

(4) $\varphi^{-1}(I)$ 非空，且 $\forall x, y \in \varphi^{-1}(I)$ 有

$$\varphi(x - y) = \varphi(x) - \varphi(y) \in I,$$

所以 $x - y \in \varphi^{-1}(I)$，即$\langle \varphi^{-1}(I), + \rangle$ 是$\langle R_1, + \rangle$ 的子群.

任取 $x \in \varphi^{-1}(I)$，$r \in R_1$，必存在 $a \in I$，$b \in R_2$，使得 $\varphi(x) = a$，$\varphi(r) = b$，那么有

$$\varphi(xr) = \varphi(x)\varphi(r) = ab \in I.$$

从而证明了 $xr \in \varphi^{-1}(I)$. 同理可证 $rx \in \varphi^{-1}(I)$，$\varphi^{-1}(I)$ 是 R_1 的理想. ∎

【例 4.13】 设 φ 是环 R_1 到 R_2 的满同态. $\ker\varphi = I$. 依照例 3.45 的方法不难证明在 R_1 的包含着 I 的理想和 R_2 的理想之间存在着一一对应.

例如 $R_1 = \langle Z, +, \cdot \rangle$ 是整数环，$R_2 = \langle Z_8, \oplus, \otimes \rangle$ 是模 8 的整数环. 令

$$\varphi: Z \to Z_8,\ \varphi(x) = (x)\text{mod}8,\ \forall x \in Z,$$

则 φ 是 R_1 到 R_2 的满同态，且 $I = \ker\varphi = 8Z$.

R_1 的包含着 I 的理想是：

$D_1 = R_1 = Z$,

$D_2 = 2Z = \{2k \mid k \in Z\}$,

$D_3 = 4Z = \{4k \mid k \in Z\}$,

$D_4 = 8Z = \{8k \mid k \in Z\}$.

R_2 的理想是：

Z_8, $\{0,2,4,6\}$, $\{0,4\}$, $\{0\}$.

令 $A_1 = \{Z, 2Z, 4Z, 8Z\}$，$A_2 = \{Z_8, \{0,2,4,6\}, \{0,4\}, \{0\}\}$. 定

义 $f: A_1 \to A_2$, $f(D) = \varphi(D)$,则

$f(Z) = Z_8$, $f(2Z) = \{0,2,4,6\}$, $f(4Z) = \{0,4\}$, $f(8Z) = \{0\}$.

f 是 A_1 和 A_2 之间的一一对应.

定理 4.8　设 D 是环 R 的理想,$g: R \to R/D$,$\forall r \in R$ 有 $g(r) = D + r$,则 g 是 R 到 R/D 的同态,且 $\ker g = D$.

证　$\forall r_1, r_2 \in R$ 有

$$g(r_1 + r_2) = D + (r_1 + r_2) = (D + r_1) + (D + r_2),$$

$$g(r_1 r_2) = D + r_1 r_2 = (D + r_1)(D + r_2).$$

g 是 R 到 R/D 的同态,$\forall r \in R$,$g(r) = D \Leftrightarrow r \in D$, 故 $\ker g = D$.

∎

称 g 是环 R 到商环 R/D 的自然同态.

定理 4.9　(环同态基本定理),环 R 的任何商环 R/D 都是 R 的同态像. 反之,若环 R' 是 R 的同态像,则 $R' \cong R/\ker\varphi$.

证　易见自然同态 $g: R \to R/D$ 是满同态.

设 $R \stackrel{\varphi}{\sim} R'$,由定理 4.6 知 $\ker\varphi$ 是 R 的理想. 如下定义 R 上的二元关系 $\sim$:$\forall a, b \in R$,$a \sim b \Leftrightarrow \varphi(a) = \varphi(b)$. 则由群同态基本定理的证明可知 $\forall a \in R$ 有 $[a] = a + \ker\varphi = \overline{a}$, 其中 $[a] \in R/\sim$, $\overline{a} \in R/\ker\varphi$. 此外 $\forall a, b \in R$ 有

$$[a] + [b] = [a + b], \quad \overline{a} + \overline{b} = \overline{a + b},$$

$$[a] \cdot [b] = [ab], \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$

所以 $\langle R/\sim, +, \cdot\rangle$ 就是 $\langle R/\ker\varphi, +, \cdot\rangle$. 由定理 1.12 得

$$R' \cong R/\ker\varphi.$$

∎

【例 4.14】　设 S 是 R 的子环,D 是 R 的理想,则

(1) $S \cap D$ 是 S 的理想;

(2) $S + D$ 是 R 的子环;

(3) $S/S \cap D \cong S + D/D$.

证　(1) 易见 $S \cap D$ 是 $\langle R, +\rangle$ 的子群,且 $\forall a \in S \cap D$,$\forall s \in S$ 有 $as \in D$ 和 $as \in S$,所以 $as \in S \cap D$. 同理可证 $sa \in S \cap D$,从

而推出 $S \cap D$ 是 S 的理想.

(2) 令 $g: R \to R/D$ 是自然映射, g 是满同态. 由于 $S + D = g^{-1}(g(S))$, 根据定理 4.7, $S + D$ 是 R 的子环.

(3) $g(S) = S + D/D$, $\ker (g \upharpoonright S) = S \cap D$, 由定理 4.9 有 $S/S \cap D \cong S + D/D$. ▮

§ 4.3 有限域上的多项式环

设 F 为域, 以 F 中元素作系数构成如下形式的多项式

$$A(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

令所有这样的多项式构成集合 S. 任取 $a(x), b(x) \in S$, 则 $a(x) + b(x), a(x)b(x) \in S$, F 上多项式加法和乘法满足交换律、结合律以及乘法对加法的分配律. 0 是零次多项式, 为 F 上多项式加法的单位元, $-a(x)$ 是 $a(x)$ 关于 F 上多项式加法的负元. 综上所述, S 关于 F 上多项式加法和乘法构成一个环. 因此我们有下面的定义.

定义 4.13 设 F 是域, 令

$$F[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in N, a_i \in F, i = 0, 1, \cdots, n\},$$

则 $F[x]$ 关于 F 上多项式的加法和乘法构成一个环, 称为**域 F 上的多项式环**. 若 F 为有限域, 则称 $F[x]$ 为**有限域 F 上的多项式环**.

定理 4.10 设 $F[x]$ 是有限域 F 上的多项式环, $f(x) \in F[x]$. 在 $F[x]$ 上如下定义二元关系 R, $\forall g(x), h(x) \in F[x]$,

$$g(x) R h(x) \Leftrightarrow f(x) \mid (g(x) - h(x)),$$

则 R 是 $F[x]$ 上的同余关系.

证 $\forall a(x) \in F[x]$, $f(x) \mid (a(x) - a(x))$, R 在 $F[x]$ 上是自反的.

$\forall a(x), b(x) \in F[x]$, 若 $a(x) R b(x)$, 则 $f(x) \mid (a(x) - b(x))$. 显然有 $f(x) \mid (b(x) - a(x))$, 所以 R 在 $F[x]$ 上是对称的.

$\forall a(x), b(x), c(x) \in F[x]$, 若 $a(x) R b(x)$, $b(x) R c(x)$, 则

$f(x)\mid(a(x)-b(x))$，$f(x)\mid(b(x)-c(x))$. 因此有

$$f(x)\mid(a(x)-b(x)+b(x)-c(x)),$$

即 $f(x)\mid(a(x)-c(x))$，所以 R 在 $F[x]$ 上是传递的. R 是 $F[x]$ 上的等价关系.

下面证明 R 关于 $F[x]$ 上的多项式加法和乘法具有置换性质.

设 $a(x),b(x),c(x),d(x)\in F[x]$，若 $a(x)Rb(x)$，$c(x)Rd(x)$，则 $f(x)\mid(a(x)-b(x))$，$f(x)\mid(c(x)-d(x))$. 因此 $f(x)$ 整除

$$(a(x)+c(x))-(b(x)+d(x)),$$

即 $(a(x)+c(x))R(b(x)+d(x))$.

令 $A(x)=a(x)c(x)-b(x)d(x)$，则

$$A(x)=(a(x)-b(x))c(x)+b(x)(c(x)-d(x)).$$

由 $f(x)\mid(a(x)-b(x))$ 和 $f(x)\mid(c(x)-d(x))$ 可知 $f(x)\mid A(x)$，所以 $a(x)c(x)Rb(x)d(x)$. ∎

由这个定理可以得到下面的定义.

定义 4.14 设 $F[x]$ 是有限域 F 上的多项式环，$f(x)\in F[x]$，$\forall g(x),h(x)\in F[x]$，若 $f(x)\mid(g(x)-h(x))$，则称 $g(x)$ 和 $h(x)$ **是模 $f(x)$ 同余的**，**记作** $g(x)\equiv h(x)(\bmod f(x))$.

【例 4.15】 $F=\{0,1\}$，则

$$F[x]=\{0,1,x,1+x,x^2,1+x^2,x+x^2,1+x+x^2,\cdots\},$$

令 $f(x)=1+x$，$g(x)=1+x+x^2$，$h(x)=x^2$，则有

$$g(x)\equiv h(x)(\bmod f(x)).$$

同时也有

$$1+x\equiv 1+x^2(\bmod f(x)),$$

$$1+x^2\equiv x+x^2(\bmod f(x))$$

等，因为在 $F[x]$ 上满足

$$(1+x)x=x+x^2.$$

【例 4.16】 设 $F[x]$ 是有限域 F 上的多项式环，$f(x)\in F[x]$. 对任意的 $a(x)\in F[x]$，根据多项式除法有下面的等式

$$a(x) = f(x)q(x) + r(x).$$

其中 $q(x)$ 为商，$r(x)$ 是余式. 如果将一个多项式中 x 最高次项的次数叫做这个多项式的次数，那么 $r(x)$ 的次数小于 $f(x)$ 的次数. 由定义 4.14 有

$$a(x) \equiv r(x)(\bmod f(x)).$$

设 $F[x]$ 是有限域 F 上的多项式环，$f(x) \in F[x]$ 是 n 次多项式，$n \geqslant 1$，将 $F[x]$ 中所有次数小于 n 的多项式构成的集合记作 $F[x]/f(x)$. 对任意的 $a(x), b(x) \in F[x]/f(x)$，如下定义 $F[x]/f(x)$ 中的**模 $f(x)$ 加法和乘法**. 若

$$a(x) + b(x) = f(x)q_1(x) + r_1(x),$$

$$a(x)b(x) = f(x)q_2(x) + r_2(x),$$

其中 $r_1(x)$ 和 $r_2(x)$ 的次数小于 $f(x)$ 的次数，则有

$$a(x) + b(x)(\bmod f(x)) = r_1(x),$$

$$a(x) \cdot b(x)(\bmod f(x)) = r_2(x).$$

易见模 $f(x)$ 加法实际上就是普通的多项式加法，因为 $a(x) + b(x)$ 的次数小于 $f(x)$ 的次数. 不难验证 $F[x]/f(x)$ 关于模 $f(x)$ 加法和乘法是封闭的，模 $f(x)$ 加法和乘法是可交换的、可结合的，并且模 $f(x)$ 乘法对模 $f(x)$ 加法是可分配的. 域 F 中的 0 和 1 分别为模 $f(x)$ 加法和乘法的单位元. $-a(x)$ 为 $a(x)$ 的负元. 因此 $F[x]/f(x)$ 关于模 $f(x)$ 加法和乘法构成一个环.

定义 4.15　设 $F[x]$ 为有限域 F 上的多项式环，$f(x) \in F[x]$ 是 n 次多项式，$n \geqslant 1$. 令

$$F[x]/f(x) = \{g(x) \mid g(x) \in F[x] \land g(x) \text{ 的次数小于 } n\},$$

则 $F[x]/f(x)$ 关于模 $f(x)$ 的加法和乘法构成一个环，称为**域 F 上的模 $f(x)$ 的多项式环**.

通常当域 $F = \{0, 1, \cdots, p-1\}$ 时将 $F[x]$ 记作 $F_p[x]$.

【例 4.17】　设 $F = \{0, 1\}$，F 上的多项式环记作 $F_2[x]$. 令 $f(x) = 1 + x + x^2$，则 F 上模 $1 + x + x^2$ 的多项式环

$$F_2[x]/(1+x+x^2)=\{0,1,x,1+x\}.$$

关于模 $1+x+x^2$ 的加法和乘法的运算表给在表 4.1 中.

表 4.1

+	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

·	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

为了给出环 $F[x]/f(x)$ 构成域的充分必要条件,我们先考虑不可约多项式.

定义 4.16 设 $F[x]$ 为域 F 上的多项式环,对任意的 $a(x)\in F[x]$,$a(x)$ 的次数为 t,如果不存在次数小于 t 且大于 0 的多项式 $b(x),c(x)\in F[x]$ 使得 $a(x)=b(x)c(x)$,则称 $a(x)$ 是**不可约的**.

例如在 $F_2[x]$ 中多项式 $1+x^3$ 不是不可约的,因为

$$1+x^3=(1+x)(1+x+x^2),$$

而 $1+x$ 和 $1+x+x^2$ 在 $F_2[x]$ 中是不可约的. 称上式为 $1+x^3$ 在 $F_2[x]$ 中分解为不可约多项式的分解式. 同一个多项式在不同的 $F[x]$ 中的分解式是不一样的. 例如 $1+x^3$ 在 $F_3[x]$ 中的分解式是

$$\begin{aligned}1+x^3&=(1+x)(1-x+x^2)\\&=(1+x)(1+2x+x^2)=(1+x)^3.\end{aligned}$$

设 F 为有限域,下面的定理给出环 $F[x]/f(x)$ 构成域的充分必要条件.

定理 4.11 设 F 为有限域,环 $F[x]/f(x)$ 是域当且仅当 $f(x)$ 在 $F[x]$ 中是不可约的.

证 必要性. 假设 $f(x)$ 在 $F[x]$ 中可约,则存在非零次多项式 $a(x),b(x)\in F[x]$,使得 $f(x)=a(x)b(x)$,且 $a(x),b(x)$ 的次数小于 $f(x)$ 的次数. 由于 $a(x),b(x)\in F[x]/f(x)$,且

$$a(x)\cdot b(x)(\mathrm{mod} f(x))=f(x)(\mathrm{mod} f(x))=0,$$

所以 $a(x),b(x)$ 是 $F[x]/f(x)$ 中的零因子，与 $F[x]/f(x)$ 是域矛盾.

充分性. 因为 F 为有限域，$f(x)$ 的次数是有限的，所以 $F[x]/f(x)$ 也是有限的. 设 $F[x]/f(x)$ 中含有 m 个多项式. 任取 $a(x)\in F[x]/f(x)-\{0\}$，若 $a(x)=1$，则 1 就是 $a(x)$ 的乘法逆元. 若 $a(x)\neq 1$，考虑 $a(x)$ 的所有乘法幂：$a(x),a^2(x),\cdots,a^m(x),\cdots$，必有

$$a^i(x)\equiv a^j(x)\ (\mathrm{mod} f(x)),\ i<j.$$

从而推出 $f(x)$ 整除 $a^j(x)-a^i(x)$，即

$$f(x)\,|\,a^i(x)(a^{j-i}(x)-1).$$

由 $a^i(x)\not\equiv 0(\mathrm{mod} f(x))$ 和 $f(x)$ 的不可约性得 $f(x)\,|\,(a^{j-i}(x)-1)$，于是有

$$a^{j-i}(x)\equiv 1\ (\mathrm{mod} f(x)).$$

易见 $j-i>1$，这就证明了 $a^{j-i-1}(x)$ 是 $a(x)$ 的逆元. 由 $a(x)$ 的任意性可知 $F[x]/f(x)$ 是域. ∎

可以证明对任何素数阶的域 $F(|F|=p)$ 和正整数 t，存在着一个 F 上的 t 次不可约多项式 $f(x)$，使得 $f(x)$ 的最高次项的系数是 1. 不难看出，$F[x]/f(x)$ 中恰含有 p^t 个元素. 根据定理 4.11，$F[x]/f(x)$ 是阶为 p^t 的域.

把以上结果和定理 4.4 结合起来就得到下面的结论：

存在阶为 n 的有限域当且仅当 n 是某个素数的幂.

习　题　四

1. 设 $*$ 和 $\circ$ 是 A 上的两个二元运算，且 $\circ$ 是可结合的，$*$ 和 $\circ$ 是互相可分配的，证明对任意 $a_1,a_2,b_1,b_2\in A$ 有

$$(a_1*b_1)\circ(a_1*b_2)\circ(a_2*b_1)\circ(a_2*b_2)$$
$$=(a_1*b_1)\circ(a_2*b_1)\circ(a_1*b_2)\circ(a_2*b_2).$$

2. 设 $Z[i]=\{a+bi \mid a,b\in Z, i=\sqrt{-1}\}$，证明 $Z[i]$ 关于复数的加法和乘法构成一个环(高斯整数环).

3. 证明 $P(B)$ 关于 $\oplus$ 和 $\cap$ 构成一个可交换的环，其中 $\oplus$ 为集合的对称差运算.

4. 在整数环中定义 $*$ 和 $\circ$ 两个二元运算. 对于任意 $a,b\in Z$ 有

$$a*b=a+b-1,$$

$$a\circ b=a+b-ab.$$

证明 $\langle Z,*,\circ\rangle$ 是一个含幺环.

5. 设 R 是环，若 $\forall a\in R$ 都有 $a^2=a$，则称 R 为布尔环. 证明

(1) R 是可交换的；

(2) $\forall a\in R$ 有 $a+a=0$；

(3) 如果 $|R|>2$，则 R 不是整环.

6. 设 R_1,R_2 是环，在 $R_1\times R_2$ 中定义两个二元运算 $*$ 和 $\circ$，对任意 $\langle a_1,b_1\rangle$，$\langle a_2,b_2\rangle\in R_1\times R_2$，

$$\langle a_1,b_1\rangle*\langle a_2,b_2\rangle=\langle a_1+a_2,\ b_1+b_2\rangle,$$

$$\langle a_1,b_1\rangle\circ\langle a_2,b_2\rangle=\langle a_1a_2,\ b_1b_2\rangle.$$

证明：

(1) $R_1\times R_2$ 关于 $*$ 和 $\circ$ 运算构成一个环；

(2) 若 R_1 和 R_2 是交换环(或含幺环)，则 $R_1\times R_2$ 也是交换环(或含幺环)；

(3) 若 R_1 和 R_2 都是整环，$R_1\times R_2$ 是整环吗?证明你的结论.

7. 设正整数 n 不是素数且 $n>1$，证明

(1) Z_n 中含有零因子；

(2) $\forall r\in Z_n, r\neq 0$，则 r 不是 Z_n 中零因子当且仅当 $(r,n)=1$；

(3) 找出 Z_{18} 中的全部零因子.

8. 设 R 为含幺环，a 是 R 中的可逆元，若 $|R|>1$，则 a 不是零因子.

9. 若 p,q 是不同的素数，证明无 pq 个元的整环.

10. 设 $\langle R,+,\cdot\rangle$ 是环，S 是 R 中所有非零因子组成的集合. 证明 $\langle S,\cdot\rangle$ 是 $\langle R,\cdot\rangle$ 的子半群. 又问 $\langle S,+,\cdot\rangle$ 是 $\langle R,+,\cdot\rangle$ 的子环吗?为什么?

11. 证明有限整环必是域.

12. 设域 F 的特征 $n\neq 0$，$a,b\in F$，证明

$$(a+b)^n = a^n + b^n.$$

13. 设 T 是域 F 的子环,且 $|T| \geqslant 2$. 令

$$S = \{ab^{-1} \mid a,b \in T,\ b \neq 0\}.$$

证明 S 是 F 中包含 T 的最小子域.

14. 设 R 是一个环,若 R 只有一个右单位元,试证 R 是含幺环.

15. 设 R 是含幺环,$u \in R$,u 有右逆元. 证明关于 u 的下述条件是等价的:

(1) u 有多于一个的右逆元;

(2) u 不是可逆的;

(3) u 是左零因子.

16. 设 R 是环,$a \in R$,若存在正整数 n 使得 $a^n = 0$,则称 a 是幂零元. 试证明 0 是整环中唯一的幂零元.

17. 设 R 是交换环,则 R 中的全体幂零元集合(见题 16) 构成 R 的子环.

18. 设 R 为交换环,证明 R 的所有幂零元的集合是 R 的一个理想.

19. 证明环 R 的两个理想的交仍是 R 的理想.

20. 设 R 是环,$A,B \subseteq R$. 令

$$A + B = \{a + b \mid a \in A \wedge b \in B\}.$$

(1) 证明当 A,B 是理想时,$A + B$ 也是理想;

(2) 举例说明当 A,B 是子环时,$A + B$ 未必是子环.

21. 设 F 是数域,证明 F 上的矩阵环 $M_n(F)$ 无非平凡理想.

22. 给出 Z_5 及 Z_6 的所有理想.

23. 设 A 是偶数环,$D = \{4x \mid x \in Z\}$. 证明 D 是 A 的一个理想,求 A/D.

24. 设 R 是交换环,D 是 R 的理想. 令

$$N(D) = \{x \mid x \in R, \text{存在正整数 } n \text{ 使 } x^n \in D\},$$

证明 $N(D)$ 是 R 的理想.

25. 设 A 是环 R 的理想,若存在正整数 n 使得

$$A^n = \{a_1a_2\cdots a_n \mid a_i \in A, i = 1,2,\cdots,n\} = \{0\},$$

则称 A 是幂零的. 证明如果环 R 有幂零理想 A,且 R/A 为幂零环,则 R 是幂零环.

26. 设 H 是环 R 的理想,且 $H \neq R$. 如果除 H 和 R 以外,R 不存在包含 H 的理想,则称 H 是 R 的极大理想. 设 R 是可交换的含幺环,证明 R/H 是域当且仅当 H 是 R 的极大理想.

27. 设 R 是交换环，$x_1, x_2, \cdots, x_m \in R$. 令

$$S = \{r_1x_1 + r_2x_2 + \cdots + r_mx_m | r_i \in R, i = 1, 2, \cdots, m\}.$$

证明 S 是 R 的理想.

28. 给出 Z_2 到 Z 的一切环同态.

29. 设 $A = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in Z\right\}$，$A$ 关于矩阵加法和乘法构成环. 证明 $B = \left\{\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \middle| x \in Z\right\}$ 是 A 的子环. 给出 A 到 B 的一个同态映射 φ，并求 $\ker\varphi$.

30. 设 $F[x]$ 是域 F 上的多项式环，令 φ: $f(x) \mapsto f(0)$，$\forall f(x) \in F[x]$. 证明 φ 是 $F[x]$ 到 F 的满同态，求 $\ker\varphi$ 和 $F[x]/\ker\varphi$.

31. 设 R 是环，A，B 是 R 的两个理想，且 $B \subseteq A$. 证明 A/B 是 R/B 的理想，且

$$R/B \Big/ (A/B) \cong R/A.$$

32. 设 φ 是环 R_1 到 R_2 的同态映射，$S \subseteq R_1$. 证明 $\varphi^{-1}(\varphi(S)) = \ker\varphi + S$.

33. 设 φ 是从域 F_1 到 F_2 的同态，且 $\varphi(F_1) \neq \{0\}$. 证明 φ 是单同态.

34. 设 G 为 Abel 群，在 $\mathrm{End}G$ 上定义两个运算. $\forall f, g \in \mathrm{End}G$,

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in G,$$

$$f \circ g(x) = f(g(x)), \quad \forall x \in G.$$

证明 $\langle \mathrm{End}G, +, \circ \rangle$ 是一个环. 称为 G 的自同态环. 设 $G = \langle a \rangle$ 是 n 阶循环群，求 G 的自同态环.

35. 证明有理数加法群的自同态环与有理数域同构.

36. 列出 $F_2[x]/(x + x^2)$ 的乘法表. $F_2[x]/(x + x^2)$ 是域吗？为什么？

37. 证明在 $F_2[x]$ 上次数大于 1 的任何不可约多项式的非零系数为奇数个.

38. 列出 $F_2[x]$ 中所有的次数从 1 到 4 的不可约多项式.

39. 在 $F_2[x]$ 中找出一个适当的不可约多项式 $f(x)$，并构造一个阶为 8 的有限域 $F_2[x]/f(x)$.

40. 将 $x^5 - 1$ 在 $F_2[x]$ 上分解为不可约多项式.

第五章　格与布尔代数

格和布尔代数是一类重要的代数系统，在计算机科学上有着广泛的应用.

§5.1　格的定义和性质

先给出格的定义.

定义 5.1　设$\langle S, \leqslant \rangle$是偏序集，若对于任意的$x, y \in S$，$\{x, y\}$都有最大下界和最小上界，则称偏序集$\langle S, \leqslant \rangle$构成一个**格**.

设x, y是格中的任意两个元素，由于$\{x, y\}$的最大下界和最小上界是唯一存在的，我们将$\{x, y\}$的最大下界记作$x \wedge y$，最小上界记作$x \vee y$.①

【例5.1】　设n为正整数，A_n为n的所有正因子的集合，则A_n关于整除关系构成格. 因为对任意$x, y \in A_n$，$x \vee y$是$[x, y]$，x与y的最小公倍数；$x \wedge y$是(x, y)，x与y的最大公约数. 而$[x, y]$和(x, y)都属于A_n. 图5.1给出了当$n = 6, 8, 30$时的格A_6, A_8, A_{30}.

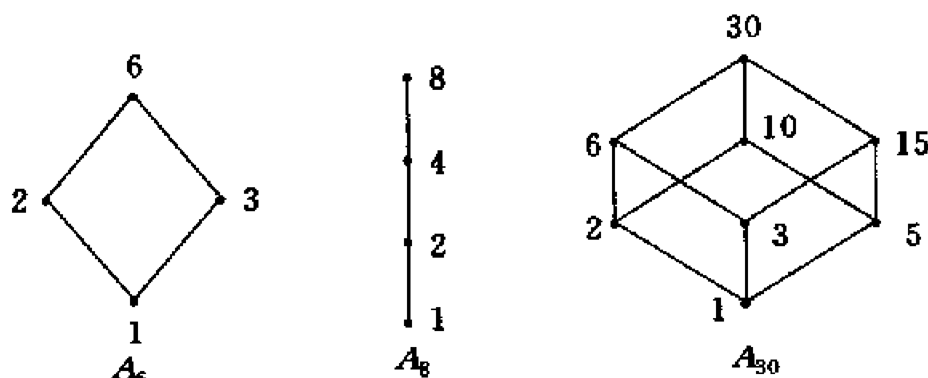


图　5.1

【例5.2】　设$P(B)$是集合B的幂集，则$P(B)$关于集合的包含关系$\subseteq$构成一个格，称为B的**幂集格**.

---

①　本章中的 $\wedge$ 和 $\vee$ 符号只代表格中求最大下界和最小上界的运算.

【例 5.3】 设 G 为群，令

$$L(G) = \{H \mid H 是 G 的子群\},$$

则 $L(G)$ 关于包含关系构成一个格，称为群 G 的**子群格**. 对于任意的 $H_1, H_2 \in L(G)$，$H_1 \wedge H_1$ 是 H_1 与 H_2 的交，也是 G 的子群，H_1 与 H_2 的最小上界是由 $H_1 \cup H_2$ 生成的子群，即 $\langle H_1 \cup H_2 \rangle$.

【例 5.4】 图 5.2 中给出的偏序集都不是格. (1) 中的 $\{e,f\}$ 没有最小上界. (2) 中的 $\{b,d\}$ 有上界 c 和 e，但没有最小上界. (3) 中的 $\{b,c\}$ 没有最小上界. (4) 中的 $\{a,e\}$ 没有上界，更没有最小上界.

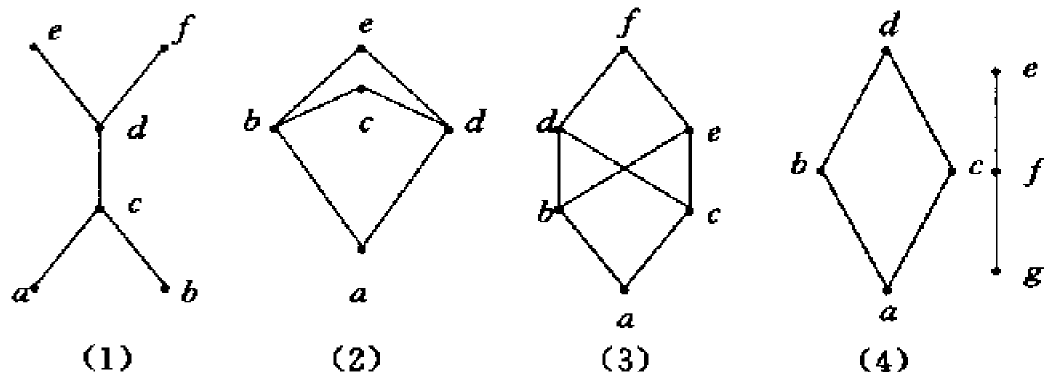


图 5.2

下面给出格的性质.

定义 5.2 设 $\langle S, \preccurlyeq \rangle$ 是格，P 是由格中元素及 $\preccurlyeq, =, \succcurlyeq, \wedge, \vee$ 等符号所表示的命题，如果将 P 中的 $\preccurlyeq, \succcurlyeq, \wedge, \vee$ 分别替换成 $\succcurlyeq, \preccurlyeq, \vee, \wedge$ 得到的命题为 P^*，称 P^* 为 P 的**对偶命题**，简称**对偶**.

例如 P 是 $a \wedge b \preccurlyeq a$，那么 P 的对偶命题 P^* 是 $a \vee b \succcurlyeq a$. 若 P 是 $a \wedge (a \vee b) = a$，那么 P 的对偶命题 P^* 是 $a \vee (a \wedge b) = a$.

格的对偶原理 如果命题 P 对一切格 L 为真，则 P 的对偶命题也对一切格为真.

证 设 P^* 为 P 的对偶，$\langle S, \preccurlyeq \rangle$ 是任意的格，只须证明 P^* 对 $\langle S, \preccurlyeq \rangle$ 为真即可. 如下定义 S 上的二元关系 $\preccurlyeq'$：$\forall a, b \in S$ 有

$$a \preccurlyeq' b \Leftrightarrow a \succcurlyeq b,$$

易证 $\preccurlyeq'$ 也是 S 上的偏序. 设任意 $a, b \in S$，$\{a,b\}$ 的最大下界和最小

上界存在，分别记作 $a \wedge' b$ 和 $a \vee' b$，并且 $a \wedge' b = a \vee b, a \vee' b = a \wedge b$. 所以 $\langle S, \preccurlyeq' \rangle$ 也是一个格，且 P^* 在 $\langle S, \preccurlyeq \rangle$ 中为真当且仅当 P 在 $\langle S, \preccurlyeq' \rangle$ 中为真. 由于命题 P 对一切格为真，所以 P^* 在 $\langle S, \preccurlyeq \rangle$ 中也为真. ∎

许多格的性质都是以对偶命题的形式成对出现. 我们只须证明其中的一个命题为真，根据对偶原理，另一命题必然为真.

定理 5.1　设 $\langle S, \preccurlyeq \rangle$ 是格，则 $\forall a,b,c \in S$ 有

(1) $a \wedge b \preccurlyeq a,\ a \wedge b \preccurlyeq b$;

(2) $a \preccurlyeq a \vee b,\ b \preccurlyeq a \vee b$;

(3) $a \preccurlyeq b$ 且 $a \preccurlyeq c \Rightarrow a \preccurlyeq b \wedge c$;

(4) $a \succcurlyeq b$ 且 $a \succcurlyeq c \Rightarrow a \succcurlyeq b \vee c$.

证　易见(2)是(1)的对偶命题，(4)是(3)的对偶命题，我们只须证明(1)和(3)即可.

(1) $\forall a,b \in S$，$a \wedge b$ 是 $\{a,b\}$ 的最大下界. 因此 $a \wedge b$ 既是 a 的下界也是 b 的下界，故有

$$a \wedge b \preccurlyeq a,\ a \wedge b \preccurlyeq b.$$

(3) $\forall a,b,c \in S$，由 $a \preccurlyeq b$ 和 $a \preccurlyeq c$ 知 a 是 $\{b,c\}$ 的下界，而 $b \wedge c$ 是 $\{b,c\}$ 的最大下界，故 $a \preccurlyeq b \wedge c$. ∎

定理 5.2　设 $\langle S, \preccurlyeq \rangle$ 是格，$\forall a,b \in S$ 有

$$a \preccurlyeq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b.$$

证　$\forall a,b \in S$，设 $a \preccurlyeq b$，由偏序 $\preccurlyeq$ 的自反性又有 $a \preccurlyeq a$. 由定理 5.1(3) 有 $a \preccurlyeq a \wedge b$. 由定理 5.1(1) 又有 $a \wedge b \preccurlyeq a$. 根据这两方面结果必有 $a \wedge b = a$.

反之，若 $a \wedge b = a$，由 $a \wedge b \preccurlyeq b$ 可得 $a \preccurlyeq b$. 综合上述就证明了 $a \preccurlyeq b \Leftrightarrow a \wedge b = a$.

同理可证　$a \preccurlyeq b \Leftrightarrow a \vee b = b$. ∎

设 $\langle S, \preccurlyeq \rangle$ 是格. 对任意的 $a,b \in S$，都有 $a \wedge b,\ a \vee b \in S$. 可以把求最大下界与最小上界看作是 S 上的两个二元运算，因此

$\langle S, \wedge, \vee \rangle$ 构成了代数系统，称为格 S 导出的代数系统. 下面讨论这个代数系统的性质.

定理 5.3　设 $\langle L, \wedge, \vee \rangle$ 是格 L 导出的代数系统，则

(1) $\forall a,b \in L$ 有

$$a \wedge b = b \wedge a,\ a \vee b = b \vee a;$$

(2) $\forall a,b,c \in L$ 有

$$(a \wedge b) \wedge c = a \wedge (b \wedge c),\ (a \vee b) \vee c = a \vee (b \vee c);$$

(3) $\forall a \in L$ 有

$$a \wedge a = a,\ a \vee a = a;$$

(4) $\forall a,b \in L$ 有

$$a \wedge (a \vee b) = a,\ a \vee (a \wedge b) = a.$$

证　根据对偶原理只须证明每条性质的前半部分.

(1) $a \wedge b$ 是 $\{a,b\}$ 的最大下界，$b \wedge a$ 是 $\{b,a\}$ 的最大下界. 由 $\{a,b\} = \{b,a\}$ 得 $a \wedge b = b \wedge a$.

(2)
$$(a \wedge b) \wedge c \preccurlyeq a \wedge b \preccurlyeq a, \quad ①$$
$$(a \wedge b) \wedge c \preccurlyeq a \wedge b \preccurlyeq b, \quad ②$$
$$(a \wedge b) \wedge c \preccurlyeq c. \quad ③$$

由 ② 和 ③ 得

$$(a \wedge b) \wedge c \preccurlyeq b \wedge c. \quad ④$$

由 ① 和 ④ 得

$$(a \wedge b) \wedge c \preccurlyeq a \wedge (b \wedge c).$$

同理可证 $a \wedge (b \wedge c) \preccurlyeq (a \wedge b) \wedge c$. 根据 $\preccurlyeq$ 的反对称性有

$$(a \wedge b) \wedge c = a \wedge (b \wedge c).$$

(3) $a \preccurlyeq a$，a 是 $\{a,a\}$ 的下界，所以 $a \preccurlyeq a \wedge a$. 又有 $a \wedge a \preccurlyeq a$，因此得 $a \wedge a = a$.

(4) 由定理 5.1(1) 有 $a \wedge (a \vee b) \preccurlyeq a$. 又由 $a \preccurlyeq a$ 和 $a \preccurlyeq a \vee b$，根据定理 5.1(3) 有 $a \preccurlyeq a \wedge (a \vee b)$，从而得到 $a \wedge (a \vee b) = a$. ▮

定理 5.3 说明格中的运算 $\wedge$ 和 $\vee$ 遵从交换律、结合律、幂等律

和吸收律.考虑一个相反的问题.能不能像群和环一样,通过规定集合、集合上的运算及运算所遵从的算律来给出格作为代数系统的定义呢?这样定义的格中的偏序是什么?而这个偏序格所导出的代数系统和原来的代数系统有什么关系?下面就来解决这些问题.

引理 设$\langle S, *, \circ\rangle$是代数系统,$*$和$\circ$是二元运算.若$*$和$\circ$是可交换、可结合、可吸收的,则

(1) $\forall a \in S$ 有 $a * a = a$, $a \circ a = a$;

(2) $\forall a, b \in S$ 有 $a \circ b = b \Leftrightarrow a * b = a$.

证 (1) $a * a = a * (a \circ (a * a)) = a$.

$$a \circ a = a \circ (a * (a \circ a)) = a.$$

(2) 必要性. $a * b = a * (a \circ b) = a$.

充分性. $a \circ b = (a * b) \circ b = b \circ (b * a) = b$. ▮

定理 5.4 设$\langle S, *, \circ\rangle$是具有两个二元运算的代数系统.若$*$和$\circ$运算遵从交换律、结合律和吸收律,则可以适当定义$S$上的偏序$\preccurlyeq$,使得$\langle S, \preccurlyeq\rangle$构成一个格,且$\langle S, \preccurlyeq\rangle$导出的代数系统$\langle S, \wedge, \vee\rangle$就是$\langle S, *, \circ\rangle$.

证 在S上定义二元关系R,$\forall a, b \in S$有

$$aRb \Leftrightarrow a \circ b = b,$$

则R为S上的偏序关系.因为根据引理有:

$\forall a \in S$ 有 $a \circ a = a$,即aRa成立,R是自反的.

$\forall a, b \in S$ 有

aRb 且 $bRa \Rightarrow a \circ b = b$ 且 $b \circ a = a \Rightarrow a = b \circ a = a \circ b = b$,

R是反对称的.

$\forall a, b, c \in S$ 有

$$aRb \text{ 且 } bRc \Rightarrow a \circ b = b \text{ 且 } b \circ c = c$$

$$\Rightarrow a \circ c = a \circ (b \circ c) = (a \circ b) \circ c = b \circ c = c \Rightarrow aRc,$$

R是传递的.

将关系R记作$\preccurlyeq$.下面证明$\forall a, b \in A$,$\{a, b\}$有最大下界和最小

上界.

$\forall a,b \in S$ 有 $a \circ b \in S$,且根据引理和已知条件得

$$a\circ(a\circ b) = (a\circ a)\circ b = a\circ b,$$

$$b\circ(a\circ b) = b\circ(b\circ a) = (b\circ b)\circ a = b\circ a = a\circ b,$$

所以 $a\circ b$ 是 $\{a,b\}$ 的一个上界.

假设 $c \in S$ 也是 $\{a,b\}$ 的上界,则 $a\circ c = c, b\circ c = c$,那么就有

$$(a\circ b)\circ c = a\circ(b\circ c) = a\circ c = c.$$

从而证明了 $a\circ b \leqslant c$,$a\circ b$ 是 $\{a,b\}$ 的最小上界.

根据引理的结论(2),类似地可以证明 $a * b$ 是 $\{a,b\}$ 的最大下界. 因此 $\langle S, \leqslant\rangle$ 构成一个格,且这个格所导出的代数系统就是 $\langle S, *, \circ\rangle$. ∎

根据定理 5.4,我们可以从代数系统的角度给出格的另一个定义.

定义 5.3　设 $\langle L, \wedge, \vee\rangle$ 是代数系统,其中 $\wedge$ 和 $\vee$ 是二元运算. 若 $\wedge$ 和 $\vee$ 运算满足交换律、结合律和吸收律,则称 $\langle L, \wedge, \vee\rangle$ 是一个格.

今后我们不再区分是偏序的格还是代数系统的格,一律统称格 L. 下面继续讨论格的性质.

定理 5.5　设 L 是格,则

(1) $\forall a,b,c \in L$ 有

$$a \leqslant b \Rightarrow a \wedge c \leqslant b \wedge c \text{ 且 } a \vee c \leqslant b \vee c;$$

(2) $\forall a,b,c,d \in L$ 有

$$a \leqslant b \text{ 且 } c \leqslant d \Rightarrow a \wedge c \leqslant b \wedge d \text{ 且 } a \vee c \leqslant b \vee d.$$

证　(1) 由 $a \wedge c \leqslant a$ 和 $a \leqslant b$ 得 $a \wedge c \leqslant b$. 而 $a \wedge c \leqslant c$,由这两个结果必有 $a \wedge c \leqslant b \wedge c$.

同理可证 $a \vee c \leqslant b \vee c$.

(2) 已知 $a \leqslant b$,由(1) 得 $a \wedge c \leqslant b \wedge c$. 同理由 $c \leqslant d$ 得 $c \wedge b \leqslant d \wedge b$. 由于 $b \wedge c = c \wedge b, d \wedge b = b \wedge d$,所以有 $a \wedge c \leqslant b \wedge d$.

同理可证 $a \vee c \leqslant b \vee d$. ∎

定理 5.5 说明格中运算 $\wedge$ 和 $\vee$ 具有保序性.

定理 5.6　设 L 是格,则

(1) $\forall a,b,c \in L$ 有

$$a \vee (b \wedge c) \leqslant (a \vee b) \wedge (a \vee c),$$
$$a \wedge (b \vee c) \geqslant (a \wedge b) \vee (a \wedge c);$$

(2) $\forall a,b,c \in L$ 有

$$a \leqslant b \Leftrightarrow a \vee (c \wedge b) \leqslant (a \vee c) \wedge b.$$

证　(1) 由对偶原理,我们只须证明第一个不等式.

由 $a \leqslant a \vee b$ 和 $a \leqslant a \vee c$ 得

$$a \leqslant (a \vee b) \wedge (a \vee c).$$

又由 $b \wedge c \leqslant b \leqslant a \vee b$ 和 $b \wedge c \leqslant c \leqslant a \vee c$ 得

$$b \wedge c \leqslant (a \vee b) \wedge (a \vee c).$$

根据定理 5.1(4) 有

$$a \vee (b \wedge c) \leqslant (a \vee b) \wedge (a \vee c).$$

(2) 必要性. 由 $a \leqslant b$ 得 $a \vee b = b$,因此有

$$a \vee (c \wedge b) \leqslant (a \vee c) \wedge (a \vee b) = (a \vee c) \wedge b.$$

充分性. $a \leqslant a \vee (c \wedge b) \leqslant (a \vee c) \wedge b \leqslant b$. ∎

以上定理中(1) 部分的不等式称为分配不等式,(2) 部分的不等式称为模不等式,当等号成立时分别称为分配律和**模律**. 对于一般的格 只成立分配不等式和模不等式,只有对某些特殊的格(分配格、模格) 才能成立分配律和模律.

§5.2　子格、格同态和格的直积

子格就是格的子代数.

定义 5.4　设 $\langle L, \wedge, \vee \rangle$ 是格,S 是 L 的非空子集. 若 S 关于运算 $\wedge$ 和 $\vee$ 是封闭的,则称 $\langle S, \wedge, \vee \rangle$ 是格 L 的**子格**.

【例 5.5】　设图 5.3 是格 L 的 Hasse 图. 令 $S_1 = \{a,e,g,h\}$,S_2

$= \{a,c,e,h\}$，则 S_1 不是 L 的子格，因为 $e \wedge g \notin S_1$，而 S_2 是 L 的子格.

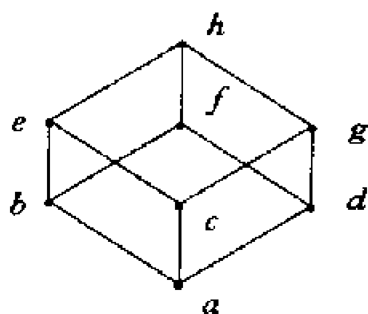


图 5.3

【例 5.6】 设 G 是群. 令 $L = P(G) = \{B \mid B \subseteq G\}$ 为 G 的幂集，则 L 关于包含关系构成一个格，即 G 的幂集格 $P(G)$. 令 $L(G) = \{H \mid H$ 是 G 的子群$\}$，则 $L(G)$ 关于包含关系构成 G 的子群格. 显然 $L(G)$ 是 $P(G)$ 的非空子集，但 $L(G)$ 不一定是 $P(G)$ 的子格. 例如 G 为 Klein 四元群 $\{e,a,b,c\}$，则子群格

$$L(G) = \{\{e\},\{e,a\},\{e,b\},\{e,c\},G\}.$$

易见 $\{e,a\}$ 和 $\{e,b\}$ 在 $P(G)$ 中的最小上界是 $\{e,a,b\}$，但 $\{e,a,b\} \notin L(G)$. $L(G)$ 关于 $P(G)$ 中运算不封闭.

下面考虑格的同态. 根据一般代数系统的同态定义不难得到格同态的定义.

定义 5.5 设 L_1, L_2 是格，$\varphi: L_1 \to L_2$. 若 $\forall a,b \in L_1$ 有 $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$ 和 $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$ 成立，则称 φ 是格 L_1 到 L_2 的**同态映射**，简称同态. 若 φ 是单射，则称 φ 为单同态；若 φ 是满射，则称 φ 是满同态；若 φ 为双射，则称 φ 是同构.

关于格的同态和同构有下面的定理.

定理 5.7 设 φ 是格 $\langle L_1, \wedge, \vee \rangle$ 到 $\langle L_2, \wedge, \vee \rangle$ 的同态映射，则 $\forall a,b \in L_1$ 有 $a \preccurlyeq b \Rightarrow \varphi(a) \preccurlyeq \varphi(b)$.

证 由 $a \preccurlyeq b$ 知 $a \wedge b = a$. 因为 φ 是 L_1 到 L_2 的同态，$\varphi(a) = \varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$. 由定理 5.2 得 $\varphi(a) \preccurlyeq \varphi(b)$. ∎

定理 5.7 说明格同态具有保序性，但其逆不一定为真，保序映射不一定是同态映射. 图 5.4 给出了三个格 L_1, L_2 和 L_3. 定义映射 φ_1, φ_2 和 φ_3.

$\varphi_1: L_1 \to L_2, \varphi_1(a) = \varphi_1(b) = \varphi_1(c) = a_1, \ \varphi_1(d) = d_1.$

$\varphi_2: L_1 \to L_2, \varphi_2(b) = \varphi_2(c) = \varphi_2(d) = d_1, \varphi_2(a) = a_1.$

$\varphi_3: L_1 \to L_3,\ \varphi_3(a) = a_2, \varphi_3(b) = b_2,\ \varphi_3(c) = c_2,\ \varphi_3(d) = d_2.$
不难看出 φ_1, φ_2 和 φ_3 都是保序映射，但它们都不是同态映射. 因为

$$\varphi_1(b \vee c) = \varphi_1(d) = d_1,\ \varphi_1(b) \vee \varphi_1(c) = a_1 \vee a_1 = a_1,$$

$$\varphi_2(b \wedge c) = \varphi_2(a) = a_1,\ \varphi_2(b) \wedge \varphi_2(c) = d_1 \wedge d_1 = d_1,$$

$$\varphi_3(b \vee c) = \varphi_3(d) = d_2,\ \varphi_3(b) \vee \varphi_3(c) = b_2 \vee c_2 = c_2.$$

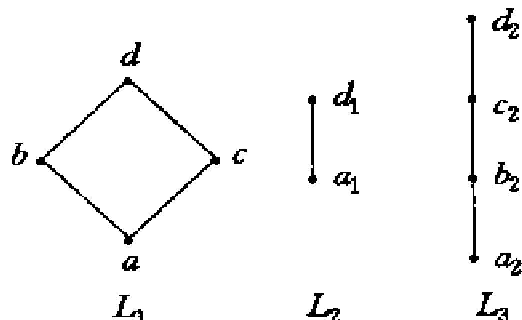


图 5.4

定理 5.8 设 L_1, L_2 是格，$\varphi: L_1 \to L_2$ 是双射，则 φ 为 L_1 到 L_2 的同构的充分必要条件是：

$$\forall a, b \in L_1,\ a \leqslant b \Leftrightarrow \varphi(a) \leqslant \varphi(b).$$

证 必要性. 由定理 5.7 有 $a \leqslant b \Rightarrow \varphi(a) \leqslant \varphi(b)$. 设 $\varphi(a) \leqslant \varphi(b)$，则 $\varphi(a) \wedge \varphi(b) = \varphi(a)$. 因为 φ 是同态，有 $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b) = \varphi(a)$. 再根据 φ 的单射性得 $a \wedge b = a$，从而有 $a \leqslant b$.

充分性. 只须证明 φ 是同态映射. $\forall a, b \in L_1$ 有 $a \leqslant a \vee b$，$b \leqslant a \vee b$. 由已知条件必有 $\varphi(a) \leqslant \varphi(a \vee b)$ 和 $\varphi(b) \leqslant \varphi(a \vee b)$，因此有

$$\varphi(a) \vee \varphi(b) \leqslant \varphi(a \vee b).$$

对 $\varphi(a) \vee \varphi(b) \in L_2$，由 φ 的满射性必存在 $d \in L_1$ 使得 $\varphi(d) = \varphi(a) \vee \varphi(b)$. 由 $\varphi(a) \leqslant \varphi(d)$ 知 $a \leqslant d$. 由 $\varphi(b) \leqslant \varphi(d)$ 知 $b \leqslant d$. 从而有 $a \vee b \leqslant d$，这就推出

$$\varphi(a \vee b) \leqslant \varphi(d) = \varphi(a) \vee \varphi(b).$$

综合这两个结果有 $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$.

同理可证 $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$. ∎

【例5.7】 设φ是格L_1到L_2的同构映射，证明φ^{-1}是格L_2到L_1的同构映射.

证 φ是双射. 由定理5.8知$\forall a,b \in L_1$有

$$a \leqslant b \Leftrightarrow \varphi(a) \leqslant \varphi(b).$$

由于φ^{-1}是L_2到L_1的双射，$\forall x,y \in L_2$必$\exists\, a,b \in L_1$使得$a = \varphi^{-1}(x)$，$b = \varphi^{-1}(y)$. 因此有

$$x \leqslant y \Leftrightarrow \varphi(a) \leqslant \varphi(b) \Leftrightarrow a \leqslant b \Leftrightarrow \varphi^{-1}(x) \leqslant \varphi^{-1}(y).$$

根据定理5.8，φ^{-1}是L_2到L_1的同构. ∎

在计算离散元素序列的极限时常常要求格是完备格. 下面给出完备格的定义以及格到完备格的嵌入定理.

设S是格L的子集，S的最大下界与最小上界分别记为$\wedge S$和$\vee S$. 若S为非空有穷集$\{a_1,a_2,\cdots,a_n\}$，则$\wedge S = a_1 \wedge a_2 \wedge \cdots \wedge a_n$，$\vee S = a_1 \vee a_2 \vee \cdots \vee a_n$. 若$S$为空集$\varnothing$，由下述条件

x是$\varnothing$的下界$\Leftrightarrow \forall a(a \in \varnothing \rightarrow x \leqslant a)$且$x \in L$，

x是$\varnothing$的上界$\Leftrightarrow \forall a(a \in \varnothing \rightarrow a \leqslant x)$且$x \in L$

可知L中任意元素都是$\varnothing$的上界和下界. 因此取$\wedge \varnothing$为L中的最大元，$\vee \varnothing$为L中的最小元. 若S为无穷集，$\wedge S$或$\vee S$可能不存在.

定义5.6 设L是格. 如果对于L的任意子集S，$\wedge S$和$\vee S$都存在，则称L是**完备格**.

有限格一定是完备格，无限格不一定是完备格. 集合B的幂集格$P(B)$是完备格，即使B是无穷集，$P(B)$也是完备格；但整数集Z关于普通的小于等于关系构成的格不是完备格.

定理5.9 设L是偏序集. 若对任意$S \subseteq L$都有$\vee S$(或$\wedge S$)存在，则L是完备格.

证 任取$S \subseteq L$，令$B = \{x | x \in L$且x是S的下界$\}$，则$B \subseteq L$. 由已知条件$\vee B$存在，令$a = \vee B$，则$\forall s \in S$有$a \leqslant s$. 所以$a \in B$，a是B中最大元，即$a = \wedge S$. 从而证明了L是完备格. 另一种情况同理可证. ∎

一个完备格的例子是格的理想格.

定义 5.7　设 I 是格 L 的非空子集,如果

(1) $\forall a,b \in I$ 有 $a \vee b \in I$,

(2) $\forall a \in I, \forall x \in L$, $x \leqslant a \Rightarrow x \in I$,

则称 I 是格 L 的一个**理想**.

格的理想是格的一个子格.因为 $\forall a,b \in I$,有 $a \wedge b \leqslant a$.由定义 5.7(2) 有 $a \wedge b \in I$,I 对 $\wedge$ 和 $\vee$ 运算都是封闭的.

【例5.8】　考虑图5.4中的格 L_1.L_1 有12个子格.它们是:$\{a\}$,$\{b\}$,$\{c\}$,$\{d\}$,$\{a,b\}$,$\{a,c\}$,$\{a,d\}$,$\{b,d\}$,$\{c,d\}$,$\{a,b,d\}$,$\{a,c,d\}$,$\{a,b,c,d\}$.其中有4个理想,即 $\{a\}$,$\{a,b\}$,$\{a,c\}$,$\{a,b,c,d\}$.

定理 5.10　设 L 是格,令

$$I(L) = \{x \mid x \text{ 是 } L \text{ 的理想}\},$$

则 $I(L)$ 关于集合的包含关系构成一个格,称为**格 L 的理想格**.

证　任取 $I_1, I_2 \in I(L)$,由于 I_1, I_2 非空,必存在 $i_1 \in I_1, i_2 \in I_2$.由于 $i_1 \wedge i_2 \leqslant i_1$,$i_1 \wedge i_2 \leqslant i_2$,即 $i_1 \wedge i_2 \in I_1$ 和 $i_1 \wedge i_2 \in I_2$.从而 $i_1 \wedge i_2 \in I_1 \cap I_2$.$I_1 \cap I_2$ 是 L 的非空子集.下面证明 $I_1 \cap I_2$ 是 L 的理想.

任取 $i,j \in I_1 \cap I_2$,则 $i,j \in I_1$ 且 $i,j \in I_2$.从而 $i \vee j \in I_1$ 和 $i \vee j \in I_2$,即 $i \vee j \in I_1 \cap I_2$.

$\forall i \in I_1 \cap I_2, \forall x \in L$,若 $x \leqslant i$,则有 $x \in I_1$ 和 $x \in I_2$,从而 $x \in I_1 \cap I_2$.

这就证明了 $I_1 \cap I_2$ 是 L 的理想.对于包含关系,$I_1 \cap I_2$ 是 $\{I_1, I_2\}$ 的最大下界.而 $\{I_1, I_2\}$ 的最小上界是包含着 $I_1 \cup I_2$ 的最小理想,因此 $I(L)$ 构成一个格. ∎

定理 5.11　对任意格 L,设 $I(L)$ 是 L 的理想格.令 $I_0(L) = I(L) \cup \{\varnothing\}$,则 $I_0(L)$ 是完备格.

证　易见 $I_0(L)$ 关于包含关系构成格,下面证明 $I_0(L)$ 是完备的.

任取 $S \subseteq I_0(L)$，若 $S=\varnothing$，则$\vee S=\varnothing\in I_0(L)$；若 $S\neq\varnothing$，则 $S=\{I_s | I_s$ 是 L 的理想，$s\in\Omega\}$，Ω 为某个指标集. 令
$A=\{a | a\in L$ 且 $a\leqslant i_{k_1}\vee i_{k_2}\vee\cdots\vee i_{k_n}, i_{k_j}\in I_{k_j},\ k_j\in\Omega, n\in Z^+\}$.
则 A 是 L 的理想. 因为 $\forall a,b\in A$ 必存在 $m,n\in Z^+$，使得

$$a\leqslant i_{k_1}\vee i_{k_2}\vee\cdots\vee i_{k_m}, i_{k_j}\in I_{k_j},\ j=1,2,\cdots,m, k_j\in\Omega,$$

$$b\leqslant i_{l_1}\vee i_{l_2}\vee\cdots\vee i_{l_n},\ i_{l_t}\in I_{l_t},\ t=1,2,\cdots,n,\ l_t\in\Omega,$$

所以

$$a\vee b\leqslant i_{k_1}\vee\cdots\vee i_{k_m}\vee i_{l_1}\vee\cdots\vee i_{l_n}.$$

易见 $a\vee b\in A$ 并且 $\forall a\in A,\forall x\in I_0(L), x\leqslant a$ 有 $x\in A$.

对任意 $I_s\in S, s\in\Omega, I_s$ 是 L 的理想. $\forall i\in I_s$，有 $i\leqslant i$，因此 $i\in A$，从而推出 $I_s\subseteq A$. A 是 S 的一个上界. 另一方面，S 的任何上界都包含有一切形如 $i_{k_1}\vee i_{k_2}\vee\cdots\vee i_{k_n}(i_{k_j}\in I_{k_j},\ k_j\in\Omega,\ n\in Z^+)$ 的元素，即 A 是 S 的最小上界，从而 $A=\vee S\in I_0(L)$. 根据定理 5.9，$I_0(L)$ 是完备格. ∎

定义 5.8　设 L_1 是格，如果能构造格 L，使得格 L_1 与 L 的某个子格同构，则称格 L_1 能**嵌入**到格 L 中.

定理 5.12　任意格 L 都可以嵌入到 $I_0(L)$ 中.

证　对任意 $a\in L$，令 $\varphi(a)=\{x | x\in L$ 且 $x\leqslant a\}$. $\forall x,y\in\varphi(a)$，则 $x\leqslant a$ 且 $y\leqslant a$，从而 $x\vee y\leqslant a$，即 $x\vee y\in\varphi(a)$. $\forall x\in\varphi(a)$，$\forall y\in L, y\leqslant x$，由 $x\leqslant a$ 得 $y\leqslant a$，即 $y\in\varphi(a)$. 这就证明 $\varphi(a)$ 是 L 的理想. $\varphi(a)\in I_0(L)$，φ 是从 L_1 到 $I_0(L)$ 的映射.

假设有 $\varphi(a)=\varphi(b)$，则

$$a\in\varphi(a)=\varphi(b)=\{x | x\in L \text{ 且 } x\leqslant b\},$$

所以有 $a\leqslant b$. 同理有 $b\leqslant a$. 由 $b=a$ 知 φ 是单射.

$\forall a,b\in L$ 有

$$\varphi(a\vee b)=\{x | x\in L \text{ 且 } x\leqslant a\vee b\}.$$

又由定理 5.11 的证明可知 $\varphi(a)\vee\varphi(b)=\{x | x\in L$ 且 $x\leqslant a\vee b\}$，这

就推出 $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$. 而

$$\begin{aligned}\varphi(a) \wedge \varphi(b) &= \{x \mid x \in L \text{ 且 } x \leqslant a\} \cap \{x \mid x \in L \text{ 且 } x \leqslant b\} \\ &= \{x \mid x \in L \text{ 且 } x \leqslant a \wedge b\} = \varphi(a \wedge b).\end{aligned}$$

所以 φ 是 L 到 $I_0(L)$ 的单同态. L 与 $\varphi(L)$ 同构. L 嵌入到 $I_0(L)$ 中. ∎

推论 任何格都可以嵌入一个完备格.

证 由定理 5.11 和 5.12 得证. ∎

下面考虑格的直积. 格的积代数仍是一个格,称为**格的直积**. 有关一般积代数的定理对格的直积都是适用的,请看下面的例子.

【例 5.9】 令 $L = \langle\{0,1\}, \leqslant\rangle$, $\leqslant$ 是通常意义下的小于等于,则 L 构成一个二元格. L 的 2 阶直积记作 L^2, 其中 $L^2 = \{\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 1,1\rangle\}$, 对任意 $\langle a,b\rangle, \langle c,d\rangle \in L^2$, $\langle a,b\rangle \leqslant \langle c,d\rangle \Leftrightarrow a \leqslant c$ 且 $b \leqslant d$. 类似地可以定义 3 阶直积 $L^3, \cdots$, 直到 n 阶直积 L^n, $n \in Z^+$. 图 5.5 给出了 L, L^2 和 L^3 的 Hasse 图.

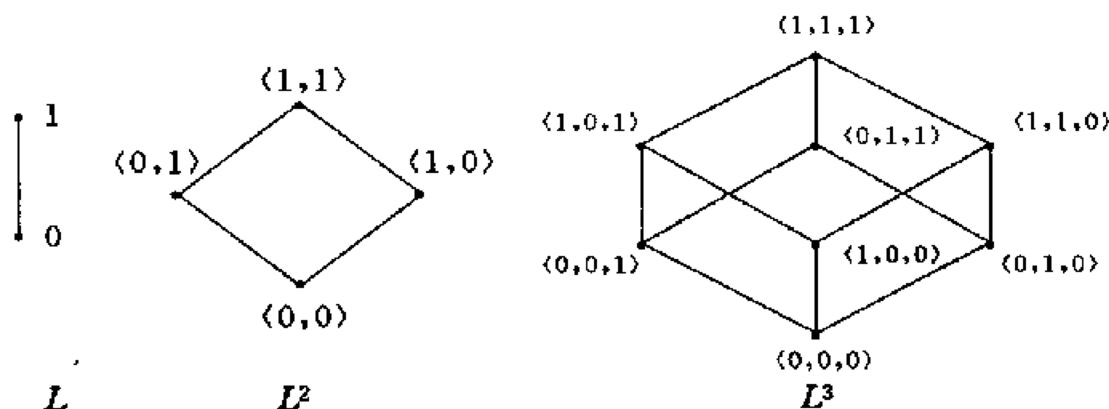


图 5.5

§5.3 模格、分配格和有补格

本节讨论几种特殊的格.

定义 5.9 设 L 是格,若 $\forall a,b,c \in L$ 有

$$a \leqslant b \Rightarrow a \vee (c \wedge b) = (a \vee c) \wedge b,$$

则称 L 为**模格**.

【例5.10】 图5.6给出了四个格 L_1, L_2, L_3, L_4，不难验证 L_1, L_2 和 L_3 都是模格，但 L_4 不是模格. 因为 $c \leqslant d$，但 $c \vee (b \wedge d) = c$，$(c \vee b) \wedge d = d$，即 $c \vee (b \wedge d) \prec (c \vee b) \wedge d$. 称 L_3 为**钻石格**，L_4 为**五角格**.

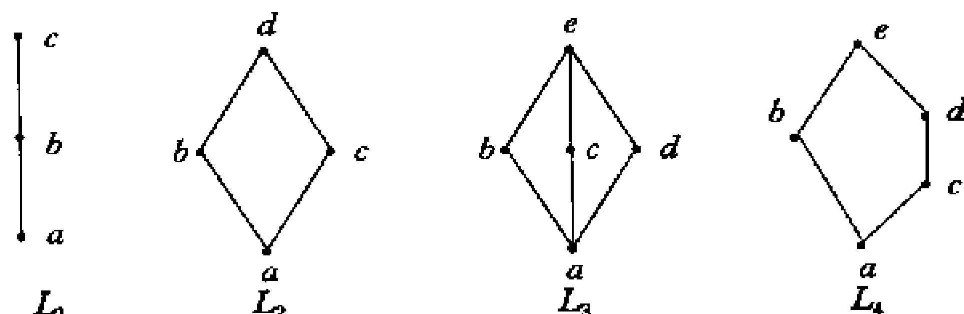


图 5.6

下面考虑一个格是模格的充要条件.

定理 5.13 一个格 L 是模格当且仅当 L 不含有和五角格同构的子格.

证 由例5.10的分析，必要性是显然的，对充分性的证明使用反证法.

假设 L 不是模格，必存在 $a,b,c \in L$，$a \prec b$ 且 $a \vee (c \wedge b) \prec (a \vee c) \wedge b$. 令 $u = c \wedge b$，$x = a \vee (c \wedge b)$，$y = (a \vee c) \wedge b$，$z = c$，$v = a \vee c$. 下面证明 $\{u,x,y,v,z\}$ 构成的子格同构于五角格.

根据 u,x,y,v,z 的定义不难得到

$$u = c \wedge b \leqslant a \vee (c \wedge b) = x \prec (a \vee c) \wedge b = y \leqslant a \vee c = v,$$

$$u = c \wedge b \leqslant c = z \leqslant a \vee c = v.$$

$\{u,x,y,v\}$ 和 $\{u,z,v\}$ 是 L 中的链. 由

$$u = u \wedge c \leqslant x \wedge c \leqslant y \wedge c = (a \vee c) \wedge b \wedge c = b \wedge c = u$$

得 $x \wedge c = y \wedge c = u$. 由

$$v = a \vee c \leqslant a \vee (c \wedge b) \vee c = x \vee c \leqslant y \vee c \leqslant a \vee c = v$$

得 $x \vee c = y \vee c = v$. 从而可知 $z = c$，$z \neq x$，$z \neq y$. 但对一切 $t,s \in \{u,x,y,v,z\}$ 都有 $t \wedge s$ 和 $t \vee s \in \{u,x,y,v,z\}$，$\{u,x,y,v,z\}$ 是 L 的子格. 由上面的分析知 x,y,z 彼此不等以及 $u \prec v$，$u \prec y$ 和 $x \prec v$.

下面证明 $z \neq v, z \neq u, x \neq u, y \neq v$.

假若 $z = v$，则有 $z \wedge y = v \wedge y = y$ 和 $z \wedge y = c \wedge y = u$，与 $u \prec y$ 矛盾. 假若 $z = u$，则有 $z \vee x = u \vee x = x$ 和 $z \vee x = c \vee x = v$，与 $x \prec v$ 矛盾.

假若 $u = x$，即 $c \wedge b = a \vee (c \wedge b)$，从而有 $a \preccurlyeq c \wedge b$. 由此得 $y = (a \vee c) \wedge b \preccurlyeq ((c \wedge b) \vee c) \wedge b = c \wedge b = u = x$，与 $x \prec y$ 矛盾.

假若 $y = v$，即 $a \vee c = (a \vee c) \wedge b$，从而有 $a \vee c \preccurlyeq b$. 由此得 $x = a \vee (c \wedge b) \succcurlyeq a \vee (c \wedge (a \vee c)) = a \vee c = v = y$，与 $x \prec y$ 矛盾.

综上所述，u, x, y, v, z 两两不等，构成 L 的 5 元子格. 令

$$\varphi: u \mapsto a,\ x \mapsto c,\ y \mapsto d,\ v \mapsto e,\ z \mapsto b,$$

则易验证 φ 是 $\{u, x, y, v, z\}$ 到图5.6中的五角格 L_4 的同构映射，与已知矛盾. ∎

定理 5.14　格 L 是模格的充要条件是对 L 中任意 $a, b, c, a \preccurlyeq b$ 有

$$a \vee c = b \vee c \text{ 且 } a \wedge c = b \wedge c \Rightarrow a = b.$$

证　充分性. 若 L 不是模格，则 L 含有一个与五角格同构的子格. 不妨设这个子格就是图 5.6 中的 L_4，则有 $b, c, d \in L, c \preccurlyeq d$，且 $c \wedge b = d \wedge b, c \vee b = d \vee b$，但 $c \neq d$，与已知矛盾.

必要性. 设 L 为模格，则有

$$\begin{aligned} a &= a \vee (a \wedge c) = a \vee (b \wedge c) = a \vee (c \wedge b) = (a \vee c) \wedge b \\ &= (b \vee c) \wedge b = b \wedge (b \vee c) = b. \end{aligned}$$

∎

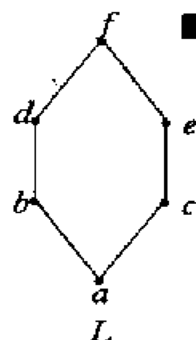


图　5.7

【例5.11】　图 5.7 中的格 L 不是模格. 令 $S = \{a, c, e, f, d\}$，则 S 是 L 的子格，且同构于五角格，由定理 5.13 可知 L 不是模格.

从另一个角度来看. 在 L 中有 $c, d, e, c \prec e$，但 $c \vee d = e \vee d$，$c \wedge d = e \wedge d$，与定理 5.14 的充要条件矛盾，因此 L 不是模格.

下面考虑分配格，先给出定义.

定义 5.10　设 L 是格，若 $\forall a,b,c \in L$ 有

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

或

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

成立，则称 L 是**分配格**.

例如图 5.6 中的 L_1 和 L_2 是分配格，但 L_3 和 L_4 不是分配格. 在 L_3 中有

$$b \wedge (c \vee d) = b \wedge e = b \text{ 和 } (b \wedge c) \vee (b \wedge d) = a \vee a = a.$$

而在 L_4 中有

$$d \wedge (b \vee c) = d \wedge e = d \text{ 和 } (d \wedge b) \vee (d \wedge c) = a \vee c = c.$$

下面给出分配格的性质.

定理 5.15　设 L 为分配格，则在 L 中成立广义分配律，即 $\forall a, b_i \in L, i = 1,2,\cdots,n$ 有

(1) $a \vee (\bigwedge_{i=1}^{n} b_i) = \bigwedge_{i=1}^{n} (a \vee b_i)$,

(2) $a \wedge (\bigvee_{i=1}^{n} b_i) = \bigvee_{i=1}^{n} (a \wedge b_i)$.

证　施归纳于 n.

(1) $n = 2$ 时显然为真.

假设 $n = k$ 时有 $a \vee (\bigwedge_{i=1}^{k} b_i) = \bigwedge_{i=1}^{k} (a \vee b_i)$ 成立，则当 $n = k+1$ 时有

$$a \vee (\bigwedge_{i=1}^{k+1} b_i) = a \vee (\bigwedge_{i=1}^{k} b_i \wedge b_{k+1}) = (a \vee (\bigwedge_{i=1}^{k} b_i)) \wedge (a \vee b_{k+1})$$

$$= \bigwedge_{i=1}^{k} (a \vee b_i) \wedge (a \vee b_{k+1}) = \bigwedge_{i=1}^{k+1} (a \vee b_i).$$

由归纳法命题得证.

(2) 同理可证. ∎

定理 5.16　设 L 为分配格，则 $\forall a,b,c \in L$ 有

$$a \wedge c = b \wedge c \text{ 且 } a \vee c = b \vee c \Rightarrow a = b.$$

证　$a = a \vee (a \wedge c) = a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

$$= (a \vee b) \wedge (b \vee c) = (b \vee a) \wedge (b \vee c) = b \vee (a \wedge c)$$
$$= b \vee (b \wedge c) = b.$$ ∎

定理 5.17　分配格一定是模格.

证　设 L 为分配格. $\forall a,b,c \in L, a \preccurlyeq b$,则有

$$a \vee (c \wedge b) = (a \vee c) \wedge (a \vee b) = (a \vee c) \wedge b,$$

L 为模格. ∎

定理 5.17 的逆不一定为真,例如钻石格是模格,但不是分配格. 下面的定理给出了模格能够构成分配格的充分必要条件.

定理 5.18　一个模格 L 是分配格当且仅当 $\forall a,b,c \in L$ 有

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a).$$

证　充分性. $\forall a,b,c \in L$ 有

$$a \wedge (b \vee c) = a \wedge (a \vee c) \wedge (b \vee c) = a \wedge (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$$
$$= a \wedge ((a \vee b) \wedge (b \vee c) \wedge (c \vee a)) = a \wedge ((a \wedge b) \vee (b \wedge c) \vee (c \wedge a))$$
$$= ((a \wedge b) \vee ((b \wedge c) \vee (c \wedge a))) \wedge a.$$

由于 $a \wedge b \preccurlyeq a$,由模律上式等于

$$(a \wedge b) \vee (((b \wedge c) \vee (c \wedge a)) \wedge a).$$

由于 $c \wedge a \preccurlyeq a$,再次使用模律得

$$(a \wedge b) \vee (c \wedge a) \vee (b \wedge c \wedge a) = (a \wedge b) \vee (a \wedge c).$$

即 $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, L 是分配格.

必要性. $\forall a,b,c \in L$ 有

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$$
$$= (((a \wedge b) \vee b) \wedge ((a \wedge b) \vee c)) \vee (c \wedge a) \quad \text{(分配律)}$$
$$= (b \wedge (a \vee c) \wedge (b \vee c)) \vee (c \wedge a) \quad \text{(吸收律,分配律)}$$
$$= (b \vee c) \wedge (b \vee a) \wedge (a \vee c \vee c) \wedge (a \vee c \vee a) \wedge (b \vee c \vee c)$$
$$\wedge (b \vee c \vee a) \quad \text{(分配律)}$$
$$= (b \vee c) \wedge (a \vee b) \wedge (c \vee a) \wedge (a \vee b \vee c) \quad \text{(幂等律,交换律)}$$
$$= (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$$ ∎

定理 5.19　一个模格是分配格当且仅当它不含有与钻石格同

构的子格.

证 必要性是显然的,只证充分性.

假设模格 L 不是分配格,必有 $a,b,c \in L$ 使得

$$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a) \prec (a\vee b)\wedge(b\vee c)\wedge(c\vee a).$$

令 $u=(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)$, $v=(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$,

$$x=u\vee(a\wedge v),\ y=u\vee(b\wedge v),\ z=u\vee(c\wedge v).$$

下面证明$\{u,v,x,y,z\}$是 L 的子格且同构于钻石格.

$$x\vee y=u\vee(a\wedge v)\vee(b\wedge v). \quad ①$$

$$a\wedge v=a\wedge(a\vee b)\wedge(b\vee c)\wedge(c\vee a)=a\wedge(b\vee c). \quad ②$$

$$b\wedge v=b\wedge(a\vee b)\wedge(b\vee c)\wedge(c\vee a)=b\wedge(c\vee a). \quad ③$$

将②和③代入①得

$$x\vee y=u\vee(a\wedge(b\vee c))\vee(b\wedge(c\vee a)). \quad ④$$

由 $a\wedge(b\vee c)\leqslant a\leqslant c\vee a$ 和模律得

$$(a\wedge(b\vee c))\vee(b\wedge(c\vee a))=((a\wedge(b\vee c))\vee b)\wedge(c\vee a). \quad ⑤$$

又由 $b\leqslant b\vee c$ 和模律有

$$(a\wedge(b\vee c))\vee b=(b\vee a)\wedge(b\vee c). \quad ⑥$$

⑥代入⑤得

$$(a\wedge(b\vee c))\vee(b\wedge(c\vee a))=(a\vee b)\wedge(b\vee c)\wedge(c\vee a)=v. \quad ⑦$$

将⑦代入④得

$$x\vee y=u\vee v=v. \quad ⑧$$

同理可证

$$x\wedge y=u. \quad ⑨$$

$$y\wedge z=z\wedge x=u. \quad ⑩$$

$$y\vee z=z\vee x=v. \quad ⑪$$

易见 $u\leqslant x\leqslant v$, $u\leqslant y\leqslant v$, $u\leqslant z\leqslant v$. 假若 $u=x$,则有 $x\vee y=u\vee y=y$,由⑧可得 $y=v$. 同理有 $z=v$,从而得到 $v=v\wedge v=y\wedge z=u$,与 $u\prec v$ 矛盾. 假若 $v=x$,则有 $x\wedge y=v\wedge y=y$,由⑨

可得 $y=u$. 同理有 $z=u$，从而 $u=u\vee u=y\vee z=v$，也与 $u\prec v$ 矛盾. 这就证明了 $u\prec x\prec v$. 类似地可以证明 $u\prec y\prec v$ 和 $u\prec z\prec v$.

假若 $x=y$，则 $x\wedge y=x$ 与 $x\wedge y=u\prec x$ 矛盾. 同理可证 x,y,z 两两不同. 因此 $\{u,v,x,y,z\}$ 是一个五元子集，且关于 $\wedge$ 与 $\vee$ 是封闭的，是 L 的子格. 若令 φ: $u\mapsto a$, $x\mapsto b$, $y\mapsto c$, $z\mapsto d$, $v\mapsto e$，不难验证 φ 是 $\{u,v,x,y,z\}$ 到例 5.10 的钻石格的同构. ∎

推论 1 格 L 是分配格当且仅当 L 既不含有与五角格同构的子格，也不含有与钻石格同构的子格.

证 由定理 5.13 和 5.19 得证. ∎

推论 2 每一条链都是分配格.

推论 3 小于五元的格都是分配格.

推论 2 和推论 3 都是推论 1 的直接结果.

有了以上的结果，我们可以将定理 5.16 强化为下面的定理.

定理 5.20 格 L 是分配格当且仅当 $\forall a,b,c\in L$ 有

$$a\wedge c=b\wedge c \text{ 且 } a\vee c=b\vee c\Rightarrow a=b.$$

证 必要性由定理 5.16 得证.

充分性. 假若 L 不是分配格，必包含一个同构于钻石格或五角格的子格. 若该子格同构于钻石格. 且它的最小元为 u，最大元为 v，其它三个元素为 x,y,z，则 $x\wedge y=z\wedge y, x\vee y=z\vee y$，但 $x\neq z$. 若该子格同构于五角格，令它的最小元为 u，最大元为 v，其它三个元为 x,y,z，且 $x\prec y$，则 $x\wedge z=y\wedge z, x\vee z=y\vee z$，但 $x\neq y$，与已知矛盾. ∎

下面考虑有界格.

定义 5.11 设 L 是一个格. 若存在 $a\in L$，使得 $\forall x(x\in L\rightarrow a\preccurlyeq x)$，则称 a 是 L 的**全下界**；若存在 $b\in L$，使得 $\forall x(x\in L\rightarrow x\preccurlyeq b)$，则称 b 是 L 的**全上界**. 如果 L 存在全上界和全下界，则称 L 是**有界格**.

格 L 的全下界实际上就是偏序集 L 的最小元，而全上界则是 L

的最大元. 而最小元和最大元如果存在,则是唯一的. 所以有界格存在着唯一的全上界和全下界,通常将全下界记为 0,全上界记为 1,而将有界格记作$\langle L,\wedge,\vee,0,1\rangle$.

【例 5.12】

(1) 钻石格和五角格都是有界格.

(2) 集合 B 的幂集格 $P(B)$ 是有界格,其中全下界是 $\varnothing$,全上界是 B.

(3) 群 G 的子群格 $L(G)$ 是有界格,其中全下界是平凡子群$\{e\}$,全上界是平凡子群 G.

(4) 完备格 L 是有界格,其中全下界是$\wedge L$,全上界是 $\vee L$.

(5) 任何有限格 L 都是有界格. 令 $L=\{a_1,a_2,\cdots,a_n\}$ 是 n 元格,则 $a_1\wedge a_2\wedge\cdots\wedge a_n$ 是 L 的全下界,$a_1\vee a_2\vee\cdots\vee a_n$ 是 L 的全上界.

由于 0 和 1 分别为格 L 中的最小元和最大元,在求一个命题 P 的对偶命题时,如果在 P 中有 0 或 1 出现,则需要将 0 换成 1,将 1 换成 0,这样才能得到正确的对偶命题 P^*. 例如命题 P 是 $a\vee 1=1$,则 P^* 是 $a\wedge 0=0$.

下面考虑有补格,先给出补元的定义.

定义 5.12 设$\langle L,\wedge,\vee,0,1\rangle$是有界格,$a\in L$. 若存在 $b\in L$ 使得 $a\vee b=1$ 和 $a\wedge b=0$,则称 b 是 a 的**补元**.

【例 5.13】 确定图 5.8 中所有格中元素的补元.

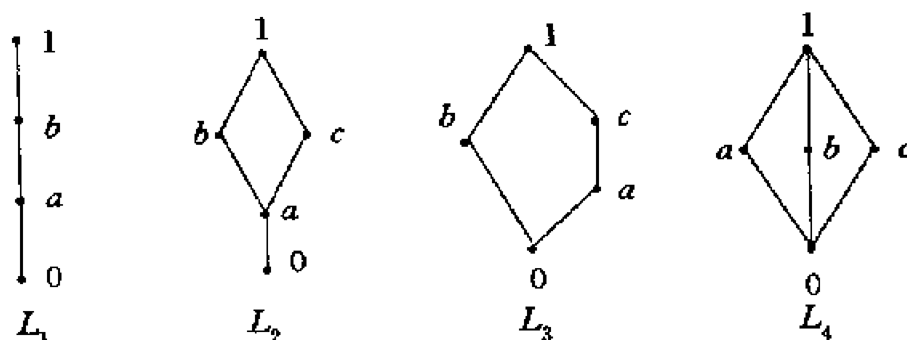


图 5.8

解 在 L_1 中,0 与 1 互为补元,a 和 b 无补元.

在 L_2 中,0 与 1 互为补元,a,b,c 无补元.

在 L_3 中,0 与 1 互为补元,a 的补元是 b,b 的补元是 a 和 c,c 的补元是 b.

在 L_4 中,0 与 1 互为补元,a 的补元是 b 和 c,b 的补元是 a 和 c,c 的补元是 a 和 b.

由这个例子可以知道在有界格 L 中 0 与 1 互为补元. 而对任何其它元素 $a \in L$,a 的补元可能不存在,如果存在也可能不是唯一的. 可以证明在分配格中如果一个元素存在补元则是唯一的.

定理 5.21　设 L 是有界分配格,$a \in L$. 若 a 存在补元,则 a 的补元是唯一的.

证　假设 b 和 c 都是 a 的补元,则有

$$a \vee b = 1, a \wedge b = 0, a \vee c = 1, a \wedge c = 0.$$

从而有 $a \vee b = a \vee c$ 和 $a \wedge b = a \wedge c$,根据定理 5.20 有 $b = c$. ∎

下面给出有补格的定义.

定义 5.13　设 $\langle L, \wedge, \vee, 0, 1\rangle$ 是有界格,若 $\forall a \in L$ 在 L 中都有 a 的补元存在,则称 L 是**有补格**.

在例 5.13 中 L_1 和 L_2 不是有补格,五角格 L_3 和钻石格 L_4 是有补格.

§5.4　布尔代数

布尔代数也叫做布尔格.

定义 5.14　一个有补分配格叫做**布尔格**(或**布尔代数**).

由上节的分析可知,在布尔格中每个元素都有唯一的补元存在,因此可以把求补运算看作是布尔格中的一元运算,记作 $-$,通常把布尔格 B 记作 $\langle B, \wedge, \vee, -, 0, 1\rangle$.

【例 5.14】　(1) 集合的幂集格 $\langle P(B), \cap, \cup, \sim, \varnothing, B\rangle$ 是布尔代数,称为**集合代数**,其中 $\cap$ 和 $\cup$ 分别为集合的交和并运算,$\sim$ 是绝对补运算(全集是 B).

(2) 逻辑代数$\langle\{0,1\},\wedge,\vee,-,0,1\rangle$是布尔代数，其中$\wedge$和$\vee$分别表示逻辑与和逻辑或，$-$是逻辑非.

从代数系统的角度可以把布尔代数看作是具有两个二元运算、一个一元运算和两个零元运算的代数系统，其中二元运算满足交换律、结合律、吸收律、幂等律、分配律，而一元运算为求补运算. 反过来，也可以通过规定集合上的运算和算律来定义一个布尔代数.

定理 5.22　设$\langle B,*,\circ,\triangle,a,b\rangle$是代数系统，其中$*$和$\circ$是二元运算，$\triangle$为一元运算，$a,b\in B$是零元运算. 如果满足以下条件：

(1) $\forall x,y\in B$有$x*y=y*x$，$x\circ y=y\circ x$，（交换律）

(2) $\forall x,y,z\in B$有

$$x*(y\circ z)=(x*y)\circ(x*z),$$
$$x\circ(y*z)=(x\circ y)*(x\circ z),$$
（分配律）

(3) $\forall x\in B$有$x*b=x$，$x\circ a=x$，（同一律）

(4) $\forall x\in B$有$x*\triangle x=a$，$x\circ\triangle x=b$，（补元律）

则$\langle B,*,\circ,\triangle,a,b\rangle$是布尔格. 若规定$*$为$B$中求最大下界运算，$\circ$为求最小上界运算，则$\triangle$为这个布尔格的求补运算且$a$是全下界0，$b$为全上界1.

证　先证$\forall x\in B$有$x\circ b=b$和$x*a=a$.

$$x\circ b=(x\circ b)*b=b*(x\circ b)=(x\circ\triangle x)*(x\circ b)=x\circ(\triangle x*b)$$
$$=x\circ\triangle x=b,$$
$$x*a=(x*a)\circ a=a\circ(x*a)=(x*\triangle x)\circ(x*a)=x*(\triangle x\circ a)$$
$$=x*\triangle x=a.$$

将$x\circ b=b$和$x*a=a$记作①式.

$\forall x,y\in B$，使用①可得

$$x\circ(x*y)=(x*b)\circ(x*y)=x*(b\circ y)=x*b=x,$$
$$x*(x\circ y)=(x\circ a)*(x\circ y)=x\circ(a*y)=x\circ a=x.$$

因此$\circ$和$*$运算满足吸收律.

为证明$\circ$和$*$运算都满足结合律，先证明以下命题：$\forall x,y,z\in$

B 有

$$x \circ y = x \circ z \text{ 且 } \triangle x \circ y = \triangle x \circ z \Rightarrow y = z. \qquad ②$$

由 $x \circ y = x \circ z$ 且 $\triangle x \circ y = \triangle x \circ z \Rightarrow (x \circ y) * (\triangle x \circ y) = (x \circ z) * (\triangle x \circ z)$

$$\Rightarrow (x * \triangle x) \circ y = (x * \triangle x) \circ z \Rightarrow a \circ y = a \circ z \Rightarrow y = z$$

命题 ② 得证.

下面证明 $\forall x,y,z \in B$ 有 $(x * y) * z = x * (y * z)$ 成立. 由等式

$$x \circ (x * (y * z)) = x, \qquad ③$$

$$x \circ ((x * y) * z) = (x \circ (x * y)) * (x \circ z) = x * (x \circ z) = x \qquad ④$$

可得 $x \circ (x * (y * z)) = x \circ ((x * y) * z).$ ⑤

而

$$\triangle x \circ (x * (y * z)) = (\triangle x \circ x) * (\triangle x \circ (y * z))$$

$$= b * (\triangle x \circ (y * z)) = \triangle x \circ (y * z), \qquad ⑥$$

$$\triangle x \circ ((x * y) * z) = (\triangle x \circ (x * y)) * (\triangle x \circ z)$$

$$= (\triangle x \circ x) * (\triangle x \circ y) * (\triangle x \circ z) = b * (\triangle x \circ y) * (\triangle x \circ z)$$

$$= (\triangle x \circ y) * (\triangle x \circ z) = \triangle x \circ (y * z). \qquad ⑦$$

由 ⑥ 和 ⑦ 有

$$\triangle x \circ (x * (y * z)) = \triangle x \circ ((x * y) * z). \qquad ⑧$$

由 ⑤ 和 ⑧,根据命题 ② 有 $x * (y * z) = (x * y) * z$,即 $*$ 运算满足结合律. 同理可证 $\circ$ 运算也满足结合律,因此 B 关于 $*$ 和 $\circ$ 运算构成一个格. 根据定理 5.4 可规定 $*$ 运算就是在格中偏序 $\preccurlyeq$ 的最大下界运算 $\wedge$,而 $\circ$ 运算就是最小上界运算 $\vee$.

由 $x * b = x$ 和 $x \circ a = x$ 知 a 是格中最小元 0,b 是格中最大元 1. 又由 $x * \triangle x = a$ 和 $x \wedge \triangle x = b$ 可知 $\triangle x$ 是 x 的补元. B 是布尔格. ▮

下面考虑布尔代数的性质.

定理 5.23　设 $\langle B, \wedge, \vee, -, 0, 1\rangle$ 是布尔代数. 则

(1) $\forall a \in B$, $\overline{\overline{a}} = a$.

(2) $\forall a,b \in B$, $\overline{a \wedge b} = \overline{a} \vee \overline{b}$, $\overline{a \vee b} = \overline{a} \wedge \overline{b}$.

(3) $\forall a,b \in B$,

$a \leqslant b \Leftrightarrow a \wedge \bar{b}=0 \Leftrightarrow \bar{a} \vee b=1 \Leftrightarrow a \wedge b=a \Leftrightarrow a \vee b=b$.

(4) $\forall a, b \in B, a \leqslant b \Leftrightarrow \bar{b} \leqslant \bar{a}$.

证 (1) $\bar{\bar{a}}$ 是 $\bar{a}$ 的补元，a 是 $\bar{a}$ 的补元，由补元唯一性有 $\bar{\bar{a}}=a$.

(2)
$$
\begin{aligned}
(a \wedge b) \vee (\bar{a} \vee \bar{b}) &= (a \vee \bar{a} \vee \bar{b}) \wedge (b \vee \bar{a} \vee \bar{b}) \\
&= (1 \vee \bar{b}) \wedge (\bar{a} \vee 1) = 1 \wedge 1 = 1, \\
(a \wedge b) \wedge (\bar{a} \vee \bar{b}) &= (a \wedge b \wedge \bar{a}) \vee (a \wedge b \wedge \bar{b}) \\
&= (0 \wedge b) \vee (a \wedge 0) = 0 \vee 0 = 0.
\end{aligned}
$$

因此 $\bar{a} \vee \bar{b}$ 是 $a \wedge b$ 的补元，由补元唯一性有 $\overline{a \wedge b}=\bar{a} \vee \bar{b}$. 同理可证

$$\overline{a \vee b}=\bar{a} \wedge \bar{b}.$$

(3) 由定理 5.2 有 $a \leqslant b \Leftrightarrow a \wedge b=a \Leftrightarrow a \vee b=b$.

证 $a \leqslant b \Rightarrow a \wedge \bar{b}=0$. $a \leqslant b \Rightarrow a \wedge \bar{b} \leqslant b \wedge \bar{b}=0 \Rightarrow a \wedge \bar{b}=0$.

证 $a \wedge \bar{b}=0 \Rightarrow \bar{a} \vee b=1$.

$$a \wedge \bar{b}=0 \Rightarrow \overline{a \wedge \bar{b}}=1 \Rightarrow \bar{a} \vee \bar{\bar{b}}=1 \Rightarrow \bar{a} \vee b=1.$$

证 $\bar{a} \vee b=1 \Rightarrow a \leqslant b$. 由 $b=0 \vee b=(a \wedge \bar{a}) \vee b=(a \vee b) \wedge (\bar{a} \vee b)$ $=(a \vee b) \wedge 1=a \vee b$ 得 $a \leqslant a \vee b=b$.

(4) $a \leqslant b \Leftrightarrow a \vee b=b \Leftrightarrow \overline{a \vee b}=\bar{b} \Leftrightarrow \bar{a} \wedge \bar{b}=\bar{b} \Leftrightarrow \bar{b} \leqslant \bar{a}$. ∎

根据一般代数系统同态映射的定义不难得到布尔代数同态的定义.

定义 5.15 设 B_1, B_2 是布尔代数，$\varphi: B_1 \to B_2$. 若 $\forall x,y \in B_1$ 有

$$
\begin{aligned}
\varphi(x \wedge y) &= \varphi(x) \wedge \varphi(y), \\
\varphi(x \vee y) &= \varphi(x) \vee \varphi(y), \\
\varphi(\bar{x}) &= \overline{\varphi(x)},
\end{aligned}
$$

则称 φ 是布尔代数 B_1 到 B_2 的**同态映射**，简称同态. 若 φ 是单射，则称 φ 是单同态；若 φ 是满射，则称 φ 是满同态；若 φ 是双射，则称 φ 是同构.

【例 5.15】 设 $A_1=\{a,b,c\}$, $A_2=\{b,c\}$, 令 $\varphi: P(A_1) \to P(A_2)$, $\varphi(x)=x-\{a\}$, $\forall x \in P(A_1)$. 则 $\forall x,y \in P(A_1)$ 有

$$\varphi(x \cup y) = (x \cup y) - \{a\} = (x - \{a\}) \cup (y - \{a\})$$
$$= \varphi(x) \cup \varphi(y),$$
$$\varphi(x \cap y) = (x \cap y) - \{a\} = (x - \{a\}) \cap (y - \{a\})$$
$$= \varphi(x) \cap \varphi(y),$$
$$\varphi(\overline{x}) = \sim x - \{a\} = (\{a,b,c\} - x) - \{a\} = \{b,c\} - x,$$
$$\overline{\varphi(x)} = \{b,c\} - \varphi(x) = \{b,c\} - (x - \{a\}) = \{b,c\} - x.$$

因此 φ 是 $P(A_1)$ 到 $P(A_2)$ 的同态,且是满同态.

不难证明布尔代数的同态具有下面的性质.

定理 5.24 设 B_1, B_2 是布尔代数,$\varphi: B_1 \to B_2$. 若 φ 是同态,则

(1) $\varphi(0) = 0$, $\varphi(1) = 1$;

(2) $\varphi(B_1)$ 是布尔代数,且是 B_2 的子代数.

证 (1) $\varphi(0) = \varphi(a \wedge \overline{a}) = \varphi(a) \wedge \varphi(\overline{a}) = \varphi(a) \wedge \overline{\varphi(a)} = 0$.

$\varphi(1) = \varphi(a \vee \overline{a}) = \varphi(a) \vee \varphi(\overline{a}) = \varphi(a) \vee \overline{\varphi(a)} = 1$.

(2) 由 $0 \in B_1$ 有 $0 = \varphi(0) \in \varphi(B_1)$,同理有 $1 \in \varphi(B_1)$,$\varphi(B_1)$ 是 B_2 的非空子集且对两个零元运算封闭.

$\forall x, y \in \varphi(B_1)$,$\exists\, a, b \in B_1$ 使得 $\varphi(a) = x$, $\varphi(b) = y$. 从而有

$$x \vee y = \varphi(a) \vee \varphi(b) = \varphi(a \vee b) \in \varphi(B_1),$$
$$x \wedge y = \varphi(a) \wedge \varphi(b) = \varphi(a \wedge b) \in \varphi(B_1).$$

$\varphi(B_1)$ 对 $\wedge$ 和 $\vee$ 运算是封闭的.

$\forall x \in \varphi(B_1)$,$\exists\, a \in B_1$ 使得 $\varphi(a) = x$,因此有

$$\overline{x} = \overline{\varphi(a)} = \varphi(\overline{a}) \in \varphi(B_1).$$

综上所述,$\varphi(B_1)$ 对 B_2 中的所有运算封闭,所以 $\varphi(B_1)$ 是 B_2 的子代数,也是布尔代数. ∎

在一个布尔代数中,0 和 1 分别为关于 $\vee$ 和 $\wedge$ 运算的单位元. 对于一般的代数系统,例如半群或独异点,只有在满同态映射下才能将单位元映到单位元. 而对群和布尔代数,只要一般的同态映射就可以做到这一点. 因为群中有着求逆元的一元运算,而布尔代数有着求补

元的一元运算. 因此在定义布尔代数同态时不必强调 $\varphi(0)=0$ 和 $\varphi(1)=1$.

下面我们来研究有限布尔代数的结构.

定义 5.16　设 L 是格, $0\in L, a\in L$. 若 $\forall b\in L$ 有

$$0\prec b\leqslant a\Rightarrow b=a,$$

则称 a 是 L 中的**原子**.

考虑图 5.8 中的几个格. 其中 L_1 的原子是 a, L_2 的原子, 也是 a, L_3 的原子是 a 和 b, L_4 的原子是 a,b,c. 若 L 是正整数 n 的全体正因子集关于整除关系构成的格, 则 L 的原子恰为 n 的所有素因子.

引理 1　设 L 是格, $a,b\in L$ 是 L 的原子. 若 $a\neq b$, 则 $a\wedge b=0$.

证　假设 $a\wedge b\neq 0$, 则有

$$0\prec a\wedge b\leqslant a \quad 和 \quad 0\prec a\wedge b\leqslant b.$$

由定义 5.16 有 $a\wedge b=a$ 和 $a\wedge b=b$, 从而得到 $a=b$, 与已知矛盾.

∎

引理 2　设 B 是有限布尔代数, $\forall x\in B, x\neq 0$, 令 $T(x)=\{a_1, a_2,\cdots,a_n\}$ 是 B 中所有小于等于 x 的原子构成的集合, 则 $x=a_1\vee a_2\vee\cdots\vee a_n$. 称这个表示式为 x 的**原子表示**, 且是唯一的表示. 这里的唯一性是指: 若 $x=a_1\vee a_2\vee\cdots\vee a_n$, $x=b_1\vee b_2\vee\cdots\vee b_m$, 则有

$$\{a_1,a_2,\cdots,a_n\}=\{b_1,b_2,\cdots,b_m\}.$$

证　令 $y=a_1\vee a_2\vee\cdots\vee a_n$. 由 $a_i\leqslant x$, $i=1,2,\cdots,n$, 有 $y\leqslant x$. 下面证明 $x\leqslant y$.

假若 $x\wedge\overline{y}\neq 0$, 则存在 B 中元素 $t_1,t_2,\cdots,t_s$, 使得 t_1 覆盖 0, t_2 覆盖 t_1, $\cdots$, t_s 覆盖 t_{s-1}, 且 $t_s=x\wedge\overline{y}$. 由此可知 t_1 是原子, 且 $t_1\leqslant x\wedge\overline{y}$, 从而有 $t_1\leqslant x$ 和 $t_1\leqslant\overline{y}$.

由 $t_1\leqslant x$ 可知 $t_1\in T(x)$, 即存在 $a_i\in T(x)$ 使得 $t_1=a_i$. 又由 $t_1\leqslant\overline{y}$ 可知 $t_1\wedge\overline{y}=t_1$, 从而有

$$t_1=t_1\wedge\overline{y}=a_i\wedge\overline{y}=a_i\wedge(\overline{a_1\vee a_2\cdots\vee a_n})$$

$$= a_i \wedge (\overline{a_1} \wedge \overline{a_2} \wedge \cdots \wedge \overline{a_n})$$
$$= (a_i \wedge \overline{a_i}) \wedge (\overline{a_1} \wedge \cdots \wedge \overline{a_{i-1}} \wedge \overline{a_{i+1}} \wedge \cdots \wedge \overline{a_n}) = 0,$$
与 t_1 覆盖 0 矛盾. 这就证明了 $x \wedge \overline{y} = 0$, 即 $x \leqslant y$. 综合上述得到 $x = a_1 \vee a_2 \vee \cdots \vee a_n$.

设 $x = b_1 \vee b_2 \vee \cdots \vee b_m$ 是 x 的另一个原子表示. 任取 $a_i \in \{a_1, a_2, \cdots, a_n\}$, 假若 $a_i \notin \{b_1, b_2, \cdots, b_m\}$, 由引理 1 必有 $a_i \wedge b_j = 0, j = 1, 2, \cdots, m$. 由于 $a_i \leqslant x$, 从而得到

$$a_i = a_i \wedge x = a_i \wedge (b_1 \vee b_2 \vee \cdots \vee b_m)$$
$$= (a_i \wedge b_1) \vee (a_i \wedge b_2) \vee \cdots \vee (a_i \wedge b_m)$$
$$= 0 \vee 0 \vee \cdots \vee 0 = 0,$$

与 a_i 是原子矛盾. 这就证明了 $a_i \in \{b_1, b_2, \cdots, b_m\}$. 同理可证, $\forall b_j \in \{b_1, b_2, \cdots, b_m\}$ 有 $b_j \in \{a_1, a_2, \cdots, a_n\}$. 于是

$$\{a_1, a_2, \cdots, a_n\} = \{b_1, b_2, \cdots, b_m\}. \qquad \blacksquare$$

定理 5.25 (有限布尔代数的表示定理)

设 B 是有限布尔代数, A 是 B 的全体原子构成的集合, 则 B 同构于 A 的幂集代数 $P(A)$.

证 $\forall x \in B$, 令 $T(x) = \{a \mid a \in B, a \text{ 是原子}, a \leqslant x\}$, 则 $T(x) \subseteq A$. 定义 $\varphi: B \to P(A)$, $\forall x \in B$, $\varphi(x) = T(x)$. 下面证明 φ 是 B 到 $P(A)$ 的同构映射.

$\forall x, y \in B$, $\forall b$, b 为原子, 有

$b \in T(x \wedge y) \Leftrightarrow b \in A,\ b \leqslant x \wedge y \Leftrightarrow b \in A,\ b \leqslant x,\ b \leqslant y$
$\Leftrightarrow (b \in A,\ b \leqslant x)$ 且 $(b \in A, b \leqslant y) \Leftrightarrow b \in T(x)$ 且 $b \in T(y)$
$\Leftrightarrow b \in T(x) \cap T(y)$.

从而有 $T(x \wedge y) = T(x) \cap T(y)$, 即 $\varphi(x \wedge y) = \varphi(x) \cap \varphi(y)$.

$\forall x, y \in B$, 设 $x = a_1 \vee a_2 \vee \cdots \vee a_n$, $y = b_1 \vee b_2 \vee \cdots \vee b_m$ 是 x 和 y 的原子表示, 则 $x \vee y = a_1 \vee \cdots \vee a_n \vee b_1 \vee \cdots \vee b_m$. 由引理 2 可知 $T(x \vee y) = \{a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m\}$. 又由于

$$T(x) = \{a_1, a_2, \cdots, a_n\},\ T(y) = \{b_1, b_2, \cdots, b_m\},$$

所以有 $T(x \vee y) = T(x) \cup T(y)$,从而得到

$$\varphi(x \vee y) = \varphi(x) \cup \varphi(y).$$

任取 $x \in B$,存在 $\bar{x} \in B$ 使得 $x \vee \bar{x} = 1$, $x \wedge \bar{x} = 0$,因此有

$$\varphi(x) \cup \varphi(\bar{x}) = \varphi(x \vee \bar{x}) = \varphi(1) = A,$$

$$\varphi(x) \cap \varphi(\bar{x}) = \varphi(x \wedge \bar{x}) = \varphi(0) = \varnothing.$$

而 A 和 $\varnothing$ 分别为 $P(A)$ 中的全上界和全下界,因此 $\varphi(\bar{x})$ 是 $\varphi(x)$ 在 $P(A)$ 中的补元,即

$$\varphi(\bar{x}) = \overline{\varphi(x)}.$$

综上所述,φ是布尔代数 B 到 $P(A)$ 的同态. 下面证明 φ是双射.

若 $\varphi(x) = \varphi(y)$,则 $T(x) = T(y) = \{a_1, a_2, \cdots, a_n\}$. 由引理 2 有 $x = a_1 \vee a_2 \vee \cdots \vee a_n = y$,于是 φ 是单射.

$\forall \{b_1, b_2, \cdots, b_m\} \in P(A)$,令 $x = b_1 \vee b_2 \vee \cdots \vee b_m$,则 $\varphi(x) = T(x) = \{b_1, b_2, \cdots, b_m\}$,$\varphi$是满射. 从而 φ是 B 到 $P(A)$ 的同构映射. ∎

定理 5.26　有限布尔代数的基数是 2^n 的形式,其中 $n \in N$,且任何两个等势的有限布尔代数都是同构的.

证　设 B 是有限布尔代数,A 是 B 的所有原子构成的集合,且 $|A| = n$. 由定理 5.25,$B \cong P(A)$,$|P(A)| = 2^n$,于是 $|B| = 2^n$.

设 B_1, B_2 是有限布尔代数, 且 $|B_1| = |B_2|$, 则 $B_1 \cong P(A_1)$, $B_2 \cong P(A_2)$, 其中 A_1, A_2 分别为 B_1 和 B_2 的原子集合. 由此得到

$$2^{|A_1|} = |P(A_1)| = |B_1| = |B_2| = |P(A_2)| = 2^{|A_2|},$$

所以有 $|A_1| = |A_2|$,存在双射 $f: A_1 \to A_2$. 令 $\varphi: P(A_1) \to P(A_2)$, $\varphi(x) = f(x)$, $\forall x \subseteq A_1$. 下面证明 φ是 $P(A_1)$ 到 $P(A_2)$ 的 同构.

$\forall x, y \in P(A_1)$, $x, y \subseteq A_1$,由集合论的知识有

$$f(x \cup y) = f(x) \cup f(y).$$

又由于 f 是单射的,$f(x \cap y) = f(x) \cap f(y)$. 从而有

$$\varphi(x \cup y) = \varphi(x) \cup \varphi(y),\ \varphi(x \cap y) = \varphi(x) \cap \varphi(y),$$

φ是 $P(A_1)$ 到 $P(A_2)$ 的同态映射.

$\forall x, y \in P(A_1)$,由于 f 是双射可得

$$\varphi(x)=\varphi(y)\Rightarrow f(x)=f(y)$$
$$\Rightarrow f^{-1}(f(x))=f^{-1}(f(y))\Rightarrow x=y,$$
因此 φ 是单射的.

$\forall y\in P(A_2)$，令 $x=f^{-1}(y)$，则由 f 是双射有 $f(x)=f(f^{-1}(y))=y$. 即 $\varphi(x)=y$，且 $x\in P(A_1)$，所以 φ 是满射的. 综合上面的结果，φ 是 $P(A_1)$ 到 $P(A_2)$ 的同构，即 $P(A_1)\cong P(A_2)$. 由同构的传递性有 $B_1\cong B_2$. ∎

为证明任何有限布尔代数都与 $\{0,1\}^n$ 同构，先给出以下引理.

引理 1 设 B 为有限布尔代数，$x,y\in B$，$x\preccurlyeq y$. 若 $x=a_1\vee a_2\vee\cdots\vee a_n$ 和 $y=b_1\vee b_2\vee\cdots\vee b_m$ 分别为 x 和 y 的原子表示，则
$$\{a_1,a_2,\cdots,a_n\}\subseteq\{b_1,b_2,\cdots,b_m\}.$$

证 令 A 是 B 的全体原子的集合. $\forall z\in B$，令 $T(z)=\{a\mid a\in A\text{ 且 }a\preccurlyeq z\}$. 定义 $\varphi: B\to P(A)$，$\varphi(z)=T(z)$，$\forall z\in B$. 由定理5.25的证明可知 φ 为 B 到 $P(A)$ 的同构. 由 $x\preccurlyeq y$ 和同构映射的保序性(定理 5.7) 有 $T(x)\subseteq T(y)$，即 $\{a_1,a_2,\cdots,a_n\}\subseteq\{b_1,b_2,\cdots,b_m\}$. ∎

引理 2 设 B 是有限布尔代数，$a\in B$ 且 $0\prec a\prec 1$. 令
$$[0,a]=\{x\mid x\in B\text{ 且 }0\preccurlyeq x\preccurlyeq a\},$$
$$[a,1]=\{x\mid x\in B\text{ 且 }a\preccurlyeq x\preccurlyeq 1\},$$
则[0,a]和[a,1]都是布尔代数，但不是 B 的子布尔代数. 其中 a 是[0,a]的全上界和[a,1]的全下界.

证 $\forall x,y\in[0,a]$，$0\preccurlyeq x\preccurlyeq a$，$0\preccurlyeq y\preccurlyeq a$ 有 $0\preccurlyeq x\vee y\preccurlyeq a$，即 $x\vee y\in[0,a]$. 而 $0\preccurlyeq x\wedge y\preccurlyeq x\preccurlyeq a$，所以 $x\wedge y\in[0,a]$. $[0,a]$ 是格.

$\forall z\in B$，令 $T(z)=\{u\mid u\text{ 是 }B\text{ 的原子且 }u\preccurlyeq z\}$.
任取 $x\in[0,a]$，$x=a_1\vee a_2\vee\cdots\vee a_n$ 和 $a=b_1\vee b_2\vee\cdots\vee b_m$ 为 x 和 a 的原子表示，则有
$$T(x)=\{a_1,a_2,\cdots,a_n\},\ T(a)=\{b_1,b_2,\cdots,b_m\}.$$

由 $x \leqslant a$ 和引理 1 有 $T(x) \subseteq T(a)$. 令 $T(y) = T(a) - T(x) = \{t_1, t_2, \cdots, t_{m-n}\}$, $y = t_1 \vee t_2 \vee \cdots \vee t_{m-n}$. 由定理 5.25 的证明可知

$$T(x \vee y) = T(x) \cup T(y) = T(a),$$
$$T(x \wedge y) = T(x) \cap T(y) = \varnothing.$$

根据原子表示的唯一性有 $x \vee y = a$ 和 $x \wedge y = 0$. 因此 x 与 y 在$[0,a]$中互为补元,其中 $0,a$ 分别为$[0,a]$的全下界和全上界. 从而证明$[0,a]$是布尔代数. 同理可证$[a,1]$也是布尔代数. ∎

定理 5.27 对每个有限布尔代数 $B, B \neq \{0\}$,都存在正整数 n,使得 $B \cong \{0,1\}^n$.

证 对 $|B|$ 进行归纳.

$|B| = 2$ 时,则 $B = \{0,1\}$,令 $n = 1$ 即可. 假设命题对一切元数小于 $|B|$ 的布尔代数为真,考虑布尔代数 B. 取 $a \in B, 0 < a < 1$,由引理 2 可知$[0,a]$和$[a,1]$是布尔代数. 令 $\varphi: B \to [0,a] \times [a,1]$, $\forall b \in B, \varphi(b) = \langle a \wedge b, a \vee b \rangle$,则 φ 为单射. 因为

$$\varphi(b_1) = \varphi(b_2) \Rightarrow \langle a \wedge b_1, a \vee b_1 \rangle = \langle a \wedge b_2, a \vee b_2 \rangle$$
$$\Rightarrow a \wedge b_1 = a \wedge b_2 \text{ 且 } a \vee b_1 = a \vee b_2 \Rightarrow b_1 = b_2.$$

对任意的$\langle x, y \rangle \in [0,a] \times [a,1]$,令 $b = y \wedge (x \vee \bar{a})$. 由 $x \leqslant a \leqslant y$ 可得

$$a \wedge b = a \wedge (y \wedge (x \vee \bar{a})) = (a \wedge y \wedge x) \vee (a \wedge y \wedge \bar{a}) = x \vee 0 = x,$$
$$a \vee b = a \vee (y \wedge (x \vee \bar{a})) = (a \vee y) \wedge (a \vee x \vee \bar{a}) = (a \vee y) \wedge 1 = y.$$

所以 $\varphi(b) = \langle x, y \rangle$, φ 是满射的.

$\forall b, c \in B$,由格的直积定义得

$$\begin{aligned}\varphi(b \vee c) &= \langle a \wedge (b \vee c), a \vee (b \vee c) \rangle = \langle (a \wedge b) \vee (a \wedge c), a \vee b \vee c \rangle \\ &= \langle a \wedge b, a \vee b \rangle \vee \langle a \wedge c, a \vee c \rangle = \varphi(b) \vee \varphi(c), \\ \varphi(b \wedge c) &= \langle a \wedge b \wedge c, a \vee (b \wedge c) \rangle = \langle a \wedge b \wedge c, (a \vee b) \wedge (a \vee c) \rangle \\ &= \langle a \wedge b, a \vee b \rangle \wedge \langle a \wedge c, a \vee c \rangle = \varphi(b) \wedge \varphi(c).\end{aligned}$$

$\varphi(\bar{b}) = \langle a \wedge \bar{b}, a \vee \bar{b} \rangle$. 由

$$(a \wedge b) \vee (a \wedge \bar{b}) = a \wedge (b \vee \bar{b}) = a,$$

$$(a \wedge b) \wedge (a \wedge \bar{b}) = 0$$

可知 $a \wedge \bar{b}$ 是 $a \wedge b$ 在$[0,a]$中的补元. 同理可证 $a \vee \bar{b}$ 是 $a \vee b$ 在$[a,1]$中的补元. 所以 $\varphi(\bar{b})$ 是 $\varphi(b)$ 在$[0,a] \times [a,1]$中的补元. 这就证明了 φ 是 B 到$[0,a] \times [a,1]$的同构.

由归纳假设存在正整数 n 和 m 使得$[0,a] \cong \{0,1\}^n$ 和$[a,1] \cong \{0,1\}^m$, 从而有

$$B \cong [0,a] \times [a,1] \cong \{0,1\}^n \times \{0,1\}^m = \{0,1\}^{n+m}. \quad \blacksquare$$

【例 5.16】 令 $A_1 = \{a\}$, $A_2 = \{a,b\}$, $A_3 = \{a,b,c\}$, 则幂集代数 $P(A_1) = \{\varnothing,\{a\}\}$ 同构于$\{0,1\}$, $P(A_2)$ 同构于$\{0,1\}^2$, 而 $P(A_3)$ 同构于$\{0,1\}^3$.

定义 5.17 设 B 是布尔代数. 函数 $f: B^n \to B$ 称为 B 上的一个 **n 元布尔函数**.

例如开关函数 $f: \{0,1\}^n \to \{0,1\}$ 是$\{0,1\}$上的 n 元布尔函数.

定理 5.28 设 B 是布尔代数, 令

$$F_n(B) = \{f \mid f: B^n \to B\}$$

是 B 上所有 n 元布尔函数的集合. $\forall f,g \in F_n(B)$, 如下定义 $f \wedge g$, $f \vee g$, $\bar{f}$, f_0 和 f_1: $\forall x \in B^n$ 有

$$(f \wedge g)(x) = f(x) \wedge g(x),$$
$$(f \vee g)(x) = f(x) \vee g(x),$$
$$\bar{f}(x) = \overline{f(x)},$$
$$f_0(x) = 0,$$
$$f_1(x) = 1.$$

则$\langle F_n(B), \wedge, \vee, -, f_0, f_1 \rangle$构成布尔代数.

证 由 B 是布尔代数易见 $\forall f,g \in F_n(B)$ 有 $f \wedge g, f \vee g, \bar{f}, f_0, f_1 \in F_n(B)$. $\forall f,g,h \in F_n(B)$, $\forall x \in B^n$ 有

$$(f \wedge g)(x) = f(x) \wedge g(x) = g(x) \wedge f(x) = (g \wedge f)(x),$$

从而推出 $f \wedge g = g \wedge f$.

同理有 $f \vee g = g \vee f$.

$$(f \wedge (g \vee h))(x) = f(x) \wedge (g \vee h)(x)$$

$$= f(x) \wedge (g(x) \vee h(x)) = (f(x) \wedge g(x)) \vee (f(x) \wedge h(x))$$

$$= (f \wedge g)(x) \vee (f \wedge h)(x) = ((f \wedge g) \vee (f \wedge h))(x),$$

从而推出 $\quad f \wedge (g \vee h) = (f \wedge g) \vee (f \wedge h)$.

同理有 $f \vee (g \wedge h) = (f \vee g) \wedge (f \vee h)$.

$$(f \wedge f_1)(x) = f(x) \wedge f_1(x) = f(x) \wedge 1 = f(x),$$

$$(f \vee f_0)(x) = f(x) \vee f_0(x) = f(x) \vee 0 = f(x),$$

从而有 $f \wedge f_1 = f$ 和 $f \vee f_0 = f$.

$$(f \wedge \overline{f})(x) = f(x) \wedge \overline{f}(x) = f(x) \wedge \overline{f(x)} = 0 = f_0(x),$$

$$(f \vee \overline{f})(x) = f(x) \vee \overline{f}(x) = f(x) \vee \overline{f(x)} = 1 = f_1(x),$$

从而有 $f \wedge \overline{f} = f_0$, $f \vee \overline{f} = f_1$.

综上所述,根据定理 5.22 可知$\langle F_n(B), \wedge, \vee, -, f_0, f_1 \rangle$构成布尔代数. ∎

考虑下面开关函数的例子.

【例 5.17】 函数 $f: \{0,1\}^n \to \{0,1\}$ 称为 n 元开关函数,令 $B = \{f \mid f: \{0,1\}^n \to \{0,1\}\}$ 是全体 n 元开关函数的集合. 定义 B 上的运算 $+, \cdot, -$ 如下: $\forall f, g \in B, \forall \langle x_1, x_2, \cdots, x_n \rangle \in \{0,1\}^n$ 有

$$(f + g)(\langle x_1, x_2, \cdots, x_n \rangle)$$

$$= f(\langle x_1, x_2, \cdots, x_n \rangle) + g(\langle x_1, x_2, \cdots, x_n \rangle),$$

$$(f \cdot g)(\langle x_1, x_2, \cdots, x_n \rangle)$$

$$= f(\langle x_1, x_2, \cdots, x_n \rangle) \cdot g(\langle x_1, x_2, \cdots, x_n \rangle),$$

$$\overline{f}(\langle x_1, x_2, \cdots, x_n \rangle) = \overline{f(\langle x_1, x_2, \cdots, x_n \rangle)},$$

则 B 和 B 上的 $+, \cdot, -$ 运算构成一个布尔代数,其中 B 的全下界为 f_0,全上界为 f_1. 任何 n 元开关函数有 2^n 种变元的组合,每个变元的组合可以对应于 0 和 1 两个值,所以有 2^{2^n} 个不同的 n 元开关函数,即 $|B| = 2^{2^n}$. 我们称这个布尔代数为**开关代数**. 开关代数是逻辑电路

的设计基础.

根据定理 5.25 的引理 2，在开关代数中每个 n 元开关函数可以唯一地写出它的原子表示. 而开关代数中的最小项就是原子，因此每个 n 元开关函数都可以唯一地表成最小项的布尔和.

习 题 五

1. 图 5.9 中给出了一些偏序集的哈斯图. 其中哪些不是格?说明理由.

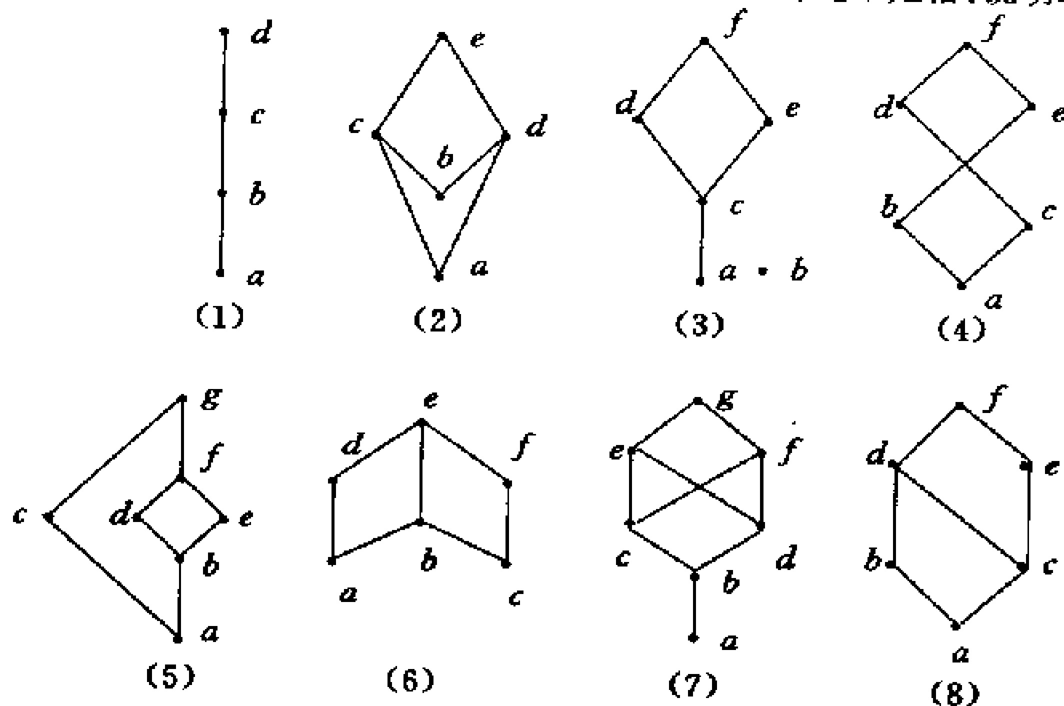


图 5.9

2. 下列各整数集合关于整除关系都构成偏序集，判断哪些偏序集是格并说明理由.

(1) $\{1,2,3,4,6\}$;

(2) $\{1,2,3,4,6,12\}$;

(3) $\{1,2,3,4,6,9,12,18,36\}$;

(4) $\{1,5,5^2,5^3,\cdots\}$.

3. 设 L 是格，$\forall a,b,c \in L, a \preccurlyeq b \preccurlyeq c$，证明

(1) $a \vee b = b \wedge c$;

(2) $(a \wedge b) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

4. 设 L 为格，证明 $\forall a,b,c,d \in L$ 有

(1) $(a \wedge b) \vee (c \wedge d) \leqslant (a \vee c) \wedge (b \vee d)$；

(2) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$.

5. 设 L 为格，$\forall a_1, a_2, \cdots, a_n \in L$，证明

$$a_1 \wedge a_2 \wedge \cdots \wedge a_n = a_1 \vee a_2 \vee \cdots \vee a_n,$$

当且仅当 $a_1 = a_2 = \cdots = a_n$.

6. 设 L 为格，$a,b \in L$. 证明 $a \wedge b \prec a$ 且 $a \wedge b \prec b$ 当且仅当 a 与 b 不可比.

7. 下面是一些关于格的命题 P，求 P 的对偶命题 P^*.

(1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$；

(2) $(a \wedge b) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$；

(3) $(a \wedge b) \vee (c \wedge d) \leqslant (a \vee c) \wedge (b \vee d)$；

(4) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$.

若 $P^* = P$，则称 P 是自对偶的. 以上命题中哪些是自对偶的？

8. 对图 5.10 的两个格 L_1 和 L_2，找出它们所有的 3 元子格、4 元子格及 5 元子格.

9. 设 L 是格，任取 $a,b \in L$，$a \prec b$. 令

$L_1 = \{x \mid x \in L \text{ 且 } x \leqslant a\}$，

$L_2 = \{x \mid x \in L \text{ 且 } a \leqslant x\}$，

$L_3 = \{x \mid x \in L \text{ 且 } a \leqslant x \leqslant b\}$.

说明 L_1, L_2, L_3 都是 L 的子格.

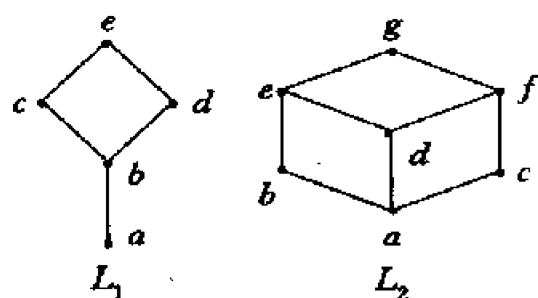


图 5.10

10. 对图 5.11 中的格，判断它们是否为模格和分配格，并说明理由.

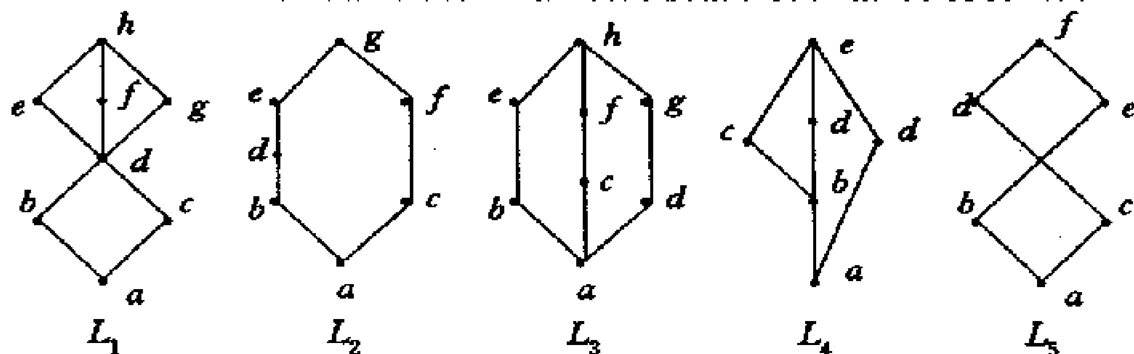


图 5.11

11. 试给出三个 6 元格，使得其中一个是分配格，一个是模格但不是分配格，一个不是模格.

12. 设 L 是格，证明 L 是模格的充分必要条件是对任意 $a,b,c \in L$ 有

$$a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c).$$

13. 设 L 是分配格，$a,b,c \in L$. 证明

$$a \wedge b \leqslant c \leqslant a \vee b \Leftrightarrow c = (a \wedge c) \vee (b \wedge c) \vee (a \wedge b).$$

14. 设 L 是模格，$a,b,c \in L$. 若有

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

成立，证明

(1) $b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c)$;

(2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

15. 设 L 是有界格，$a,b \in L$，证明

(1) 若 $a \vee b = 0$，则 $a = b = 0$;

(2) 若 $a \wedge b = 1$，则 $a = b = 1$.

16. 设 L 为有限格，证明

(1) 若 $|L| \geqslant 2$，则 L 中不存在以自身为补元的元素；

(2) 若 $|L| \geqslant 3$ 且 L 是一条链，则 L 不是有补格.

17. 设 L 是有界分配格，L_1 是 L 中所有具有补元的元素构成的集合，证明 L_1 是 L 的子格.

18. 给出所有的 5 元格，并说明哪些是模格，哪些是分配格，哪些是有补格.

19. 设 L 是长为 n 的链，$G = \langle a \rangle$ 是 p^t 阶循环群，p 是素数. 若 $n = t + 1$，证明 L 与 G 的子群格同构.

20. 设 L 是分配格，$a \in L$. 令

$$f(x) = x \vee a,\ g(x) = x \wedge a,\ \forall x \in L.$$

证明 f 和 g 都是格 L 的自同态映射并求出这两个自同态的同态像.

21. 设 L 是分配格，$a,b \in L$，令

$$X = \{x \mid x \in L \text{ 且 } a \wedge b \leqslant x \leqslant a\},$$
$$Y = \{y \mid y \in L \text{ 且 } b \leqslant y \leqslant a \vee b\}.$$

定义 $f(x) = x \vee b,\ \forall x \in X,\ g(y) = y \wedge a,\ \forall y \in Y$. 证明 f 和 g 是 X 与 Y 之间一对互逆的格同构映射.

22. 设 L 是格，A 是 L 的所有自同态映射构成的集合. 证明 A 关于映射的合

成运算∘构成一个独异点.

23. 设 $L = \{0,a,b,c,1\}$ 是钻石格，找出 L 所有的理想，并给出 L 的理想格 $I(L)$ 的哈斯图.

24. 证明对有限格 L 有 $I(L) \cong L$.

25. 设 $L_1 = \{0,a,1\}$，$L_2 = \{0,1\}$，做出格的直积 $L_1 \times L_2$ 和 $L_1 \times L_2 \times L_2$ 的哈斯图.

26. 设 $\langle B,\wedge,\vee,-,0,1\rangle$ 是布尔代数，证明 $\forall a,b \in B$ 有

(1) $a \vee (\bar{a} \wedge b) = a \vee b$;

(2) $a \wedge (\bar{a} \vee b) = a \wedge b$.

27. 设 $\langle B,\wedge,\vee,-,0,1\rangle$ 是布尔代数. 在 B 上定义二元运算 $\oplus$ 如下：$\forall a,b \in B$,

$$a \oplus b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b).$$

证明 $\langle B,\oplus\rangle$ 构成 Abel 群.

28. 设 $\langle B,\wedge,\vee,-,0,1\rangle$ 是布尔代数. 在 B 上定义二元运算 $\oplus$ 和 $\otimes$. $\forall a,b \in B$ 有

$$a \oplus b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b),$$

$$a \otimes b = a \wedge b.$$

证明 $\langle B,\oplus,\otimes\rangle$ 是一个布尔环(布尔环定义见习题四题 5).

29. 设 B 是有限布尔代数，$A = \{a_1,a_2,\cdots,a_n\}$ 是 B 的全体原子的集合. 证明 $\forall x \in B$，$x = 0$ 当且仅当对每个 i，$i = 1,2,\cdots,n$ 有 $x \wedge a_i = 0$.

30. 设 B 是布尔代数，$a_1,a_2,\cdots,a_n \in B$，证明

(1) $\overline{a_1 \wedge a_2 \wedge \cdots \wedge a_n} = \overline{a_1} \vee \overline{a_2} \vee \cdots \vee \overline{a_n}$;

(2) $\overline{a_1 \vee a_2 \vee \cdots \vee a_n} = \overline{a_1} \wedge \overline{a_2} \wedge \cdots \wedge \overline{a_n}$.

31. 设 B 是布尔代数，$a,b,c \in B$，在 B 中化简以下表达式：

(1) $(a \wedge b) \vee (a \wedge \bar{b}) \vee (\bar{a} \vee b)$;

(2) $(a \wedge b) \vee (a \wedge \overline{b \wedge c}) \vee c$.

32. 设 B_1,B_2 是两个布尔代数，$\varphi: B_1 \to B_2$. 若对任意 $a,b \in B_1$ 有

$$\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b), \quad \varphi(\bar{a}) = \overline{\varphi(a)},$$

证明 φ 是 B_1 到 B_2 的同态.

33. 设 B 是布尔代数，$a,b \in B$ 且 $a \prec b$. 令

$$[a,b] = \{x \mid x \in B \text{ 且 } a \leqslant x \leqslant b\}.$$

证明$[a,b]$也是一个布尔代数. 问$[a,b]$是否为B的子布尔代数?

34. 设φ是有限布尔代数B_1到B_2的同构,证明

(1) 若a是B_1中的原子,则$\varphi(a)$是B_2中的原子;

(2) 2^n个元素的布尔代数有且仅有n个原子.

35. 设φ是布尔代数B_1到B_2的同态映射,令

$$J = \varphi^{-1}(0) = \{x \mid x \in B_1 \text{ 且 } \varphi(x) = 0\}.$$

试证明

(1) $0 \in J$;

(2) 若$a \in J$,则对任意的$x \in B_1$,只要$x \leqslant a$,就有$x \in J$;

(3) 对任意$a,b \in J$有$a \vee b \in J$.

36. 设$B_1 = \{0,a,b,1\}$是4元布尔代数,其中$a = \bar{b}$. $B_2 = \{0,1\}$也是布尔代数.

(1) 给出B_1到B_2的所有布尔代数同态,并求出每个同态的同态像;

(2) 令φ: $B_1 \to B_2$是布尔代数同态,设φ在B_1上导出的同余关系为$\sim$. 试描述由(1)中的布尔代数同态所确定的商布尔代数$B_1/\sim$,说明$B_1/\sim$的集合和运算.

37. 设A,B是两个不交的集合. 试证明: 集合代数$\langle P(A \cup B), \cap, \cup, \sim, \varnothing, A \cup B\rangle$同构于$\langle P(A) \times P(B), \wedge, \vee, -, \langle\varnothing,\varnothing\rangle, \langle A,B\rangle\rangle$,其中$\forall X_1, X_2, X \subseteq A$, $Y_1, Y_2, Y \subseteq B$有

$$\langle X_1,Y_1\rangle \wedge \langle X_2,Y_2\rangle = \langle X_1 \cap X_2,\ Y_1 \cap Y_2\rangle,$$
$$\langle X_1,Y_1\rangle \vee \langle X_2,Y_2\rangle = \langle X_1 \cup X_2,\ Y_1 \cup Y_2\rangle,$$
$$-\langle X,Y\rangle = \langle A - X, B - Y\rangle.$$

38. 设φ是布尔代数B_1到B_2的满同态映射,$\sim$是φ导出的B_1上的同余关系. g: $B_1 \to B_1/\sim$是自然映射,$\forall x \in B_1$, $g(x) = [x] = \{y \mid y \in B_1 \text{ 且 } \varphi(y) = \varphi(x)\}$. 证明存在唯一的同构映射$f$: $B_1/\sim \to B_2$使得$f \circ g = \varphi$.

39. 找出8元布尔代数的所有子代数.

40. 设B是有限布尔代数,且$|B| > 2$. 任取$x \in B$,证明$\{0,x,\bar{x},1\}$是B的子布尔代数.

第二篇
组 合 数 学

第六章　组合存在性定理

组合存在性定理主要有 Ramsey 定理，偏序集的分解定理以及相异代表系存在定理. 有关偏序集的分解定理已在集合论中做过介绍，这里不再重复. 本章将简要地讨论其它两个存在性定理及应用.

§6.1　鸽巢原理和 Ramsey 定理

鸽巢原理也叫做**抽屉原则**，是 Ramsey 定理的特例. 先给出鸽巢原理的简单形式.

定理 6.1　（鸽巢原理）把 $n+1$ 个物体放入 n 个盒子里，则至少有一个盒子里含有两上或两上以上的物体.

证　假设每个盒子里至多一个物体，则 n 个盒子里的物体总数小于等于 n，与物体总数是 $n+1$ 矛盾. ▮

【例 6.1】　用两种颜色涂图 6.1 中的 9×3 方格，每个方格涂一种颜色. 证明必有两列的涂色是相同的.

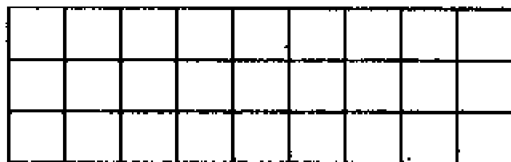


图　6.1

证　每个列可能的涂色方案为 $2^3=8$ 种. 由鸽巢原理 9 个列中必有两列涂色方案相同. ▮

【例 6.2】　证明 n 个连续整数中至少有一个数能被 n 整除.

证　设 n 个连续整数为 $x_1,x_2,\cdots,x_n$. 对于 $i=1,2,\cdots,n$，由除法有 $x_i=n\cdot g_i+r_i$，其中 $r_i\in\{0,1,\cdots,n-1\}$. 假若存在 $r_j=0$，$j\in\{1,2,\cdots,n\}$，则 x_j 可以被 n 整除. 若不然，由鸽巢原理必有 $r_t=r_s$，$t,s\in\{1,2,\cdots,n\}$，$t<s$. 则 $n\mid(x_s-x_t)$，即 $x_s-x_t\geqslant n$，与 $x_1,x_2,\cdots,x_n$ 是连续整数矛盾. ▮

【例 6.3】　设 $x_1,x_2,\cdots,x_n$ 是 n 个正整数，证明其中存在着连续的若干个数，其和是 n 的倍数.

证 令 $S_i = x_1 + x_2 + \cdots + x_i$，$S_i$ 除以 n 的余数记作 r_i，$i = 1,2,\cdots,n$. 若存在某个 $r_i = 0$，则 $x_1 + x_2 + \cdots + x_i$ 可以被 n 整除. 否则由鸽巢原理必有 $r_k = r_j$，$j > k$，因此

$$S_j - S_k = x_{k+1} + x_{k+2} + \cdots + x_j$$

可以被 n 整除. ∎

【例 6.4】 证明在 $n+1$ 个小于等于 $2n$ 且互不相等的正整数中必有两个数互素.

证 先证明以下的事实：

任何两个相邻的正整数是互素的.

用反证法，假设 n 与 $n+1$ 有公因子 $q(q \geqslant 2)$，则有

$$n = qp_1, \quad n+1 = qp_2, \quad p_1, p_2 \text{ 是整数}.$$

从而有 $qp_1 + 1 = qp_2$，即 $q(p_2 - p_1) = 1$. 这与 $q \geqslant 2$，$p_2 - p_1$ 是整数矛盾.

把 $1,2,\cdots,2n$ 分成以下 n 个组：

$$\{1,2\},\{3,4\},\cdots,\{2n-1,2n\}.$$

从组中任取 $n+1$ 个不同的数，由鸽巢原理必有两个数取自同一组. 它们是相邻的数，所以它们是互素的. ∎

【例 6.5】 在 $1,2,\cdots,2n$ 中任取 $n+1$ 不同的数，证明至少有一个数是另一个数的倍数.

证 任何的正整数 n 都可以表成 $n = 2^{\alpha} \cdot \beta$ 的形式，其中 α 是自然数(包括 0)，β 为奇数.

设选出的 $n+1$ 个数从小到大依次为 $a_1, a_2, \cdots, a_{n+1}$. 设 $a_i = 2^{\alpha_i} \cdot \beta_i$，$i = 1,2,\cdots,n+1$. $\beta_1, \beta_2, \cdots, \beta_{n+1}$ 只可能取值为 $1,3,\cdots,2n-1$. 由鸽巢原理必有 $\beta_i = \beta_j$，$i < j$，因此有

$$\frac{a_j}{a_i} = \frac{2^{\alpha_j} \cdot \beta_j}{2^{\alpha_i} \cdot \beta_i} = 2^{\alpha_j - \alpha_i},$$

从而证明 a_j 是 a_i 的倍数. ∎

【例 6.6】 一个棋手为参加一次锦标赛将进行 77 天的练习. 如

果他每天至少下一盘棋，而每周至多下 12 盘棋，证明存在着一个正整数 n 使得他在这 77 天里有连续的 n 天共下了 21 盘棋.

证 设 a_i 是从第 1 天到第 i 天下棋的总盘数，$i = 1, 2, \cdots, 77$. 因为他每天至少下一盘棋，所以

$$1 \leqslant a_1 < a_2 < \cdots < a_{77}.$$

又因为每周至多下 12 盘棋，77 天中下棋的总数

$$a_{77} \leqslant 12 \times \frac{77}{7} = 132.$$

做序列

$$a_1 + 21,\ a_2 + 21, \cdots, a_{77} + 21,$$

这个序列也是严格单调上升的，且 $a_{77} + 21 \leqslant 153$. 考察下面的序列：

$$a_1, a_2, \cdots, a_{77}, a_1 + 21, a_2 + 21, \cdots, a_{77} + 21,$$

该序列有 154 个数，每个数都是小于等于 153 的正整数. 由鸽巢原理必存在 i 和 j，$j < i$，使得 $a_i = a_j + 21$. 令 $n = i - j$，则该棋手在第 $j+1, j+2, \cdots, j+n = i$ 的连续 n 天内下了 21 盘棋. ▮

下面考虑鸽巢原理的一般形式.

定理 6.2 （鸽巢原理的一般形式）

设 $q_1, q_2, \cdots, q_n$ 是给定的正整数，若把 $q_1 + q_2 + \cdots + q_n - n + 1$ 个物体放入 n 个盒子里，则或第一个盒子至少包含了 q_1 个物体，或第二个盒子至少包含了 q_2 个物体，…，或第 n 个盒子至少包含了 q_n 个物体.

证 假若第 i 个盒子至多包含 $q_i - 1$ 个物体，$i = 1, 2, \cdots, n$，则盒子里的物体总数至多是

$$q_1 + q_2 + \cdots + q_n - n,$$

与物体总数为 $q_1 + q_2 + \cdots + q_n - n + 1$ 矛盾. ▮

推论 若 $n(r-1)+1$ 个物体放入 n 个盒子里，则至少有一个盒子里含有 r 个或者更多的物体.

证 在定理 6.2 中令 $q_1 = q_2 = \cdots = q_n = r$ 即可. ∎

若令推论中的 $r = 2$,就得到鸽巢原理的简单形式.所以鸽巢原理的一般形式是简单形式的推广,简单形式是一般形式的特例.

定理 6.3 (鸽巢原理的算术平均形式)

设 $m_1, m_2, \cdots, m_n$ 是 n 个正整数,如果它们的算术平均

$$(m_1 + m_2 + \cdots + m_n)/n > r - 1,$$

则存在 $m_i \geqslant r$,其中 $i \in \{1, 2, \cdots, n\}$.

证 由已知条件得

$$m_1 + m_2 + \cdots + m_n \geqslant (r - 1)n + 1.$$

根据定理 6.2 的推论可知存在 $m_i \geqslant r, i \in \{1, 2, \cdots, n\}$. ∎

定理 6.4 (鸽巢原理的函数形式)

设 $f: A \to B$,其中 $|A| = m$, $|B| = n$, $m, n \in Z^+$.若 $m > n$,则在 A 中至少存在$\lceil m/n \rceil$个元素 $a_1, a_2, \cdots, a_{\lceil m/n \rceil}$ 使得 $f(a_1) = f(a_2) = \cdots = f(a_{\lceil m/n \rceil})$.其中$\lceil m/n \rceil$表示大于等于$m/n$的最小正整数.

证 令 $m_1 + m_2 + \cdots + m_n = m$, $B = \{y_1, y_2, \cdots, y_n\}$,其中 m_i 表示函数值等于 y_i 的自变量个数.由 $m/n > \lceil m/n \rceil - 1$ 得

$$(m_1 + m_2 + \cdots + m_n)/n > \lceil m/n \rceil - 1.$$

根据定理 6.3,必存在某个 $m_i \geqslant \lceil m/n \rceil$,即在 A 中至少存在$\lceil m/n \rceil$个元素 $a_1, a_2, \cdots, a_{\lceil m/n \rceil}$,使得 $f(a_1) = f(a_2) = \cdots = f(a_{\lceil m/n \rceil})$.

∎

【例 6.7】 有大小两个圆盘,把它们各分成 200 个相等的扇形.从大盘上任选 100 个扇形涂上红色,其余的涂上蓝色.而在小盘的每个小扇形中任意涂上红色或蓝色,然后将小盘放到大盘上,并使两个盘的圆心重合.证明在旋转小盘时可以找到某个位置使得至少有 100 个小扇形落在同样颜色的大扇形内. ∎

证 任取一个小扇形,当它落入某个大扇形的内部以后,这两个扇形的颜色就构成一组颜色组合.在小盘旋转一周的过程中,这个

小扇形与大盘上所有的扇形共构成 200 组颜色组合，其中同色的有 100 组. 因为小盘上有 200 个不同的扇形，所有的小扇形与所有的大扇形构成的同色的颜色组合总共有 $100 \times 200 = 20000$ 组. 而小盘与大盘的相对位置有 200 种，每种位置平均具有 $20000/200 = 100$ 组同色的颜色组合. 由定理 6.3，必存在着某个位置使得至少有 100 个小扇形落到同色的大扇形内. ∎

【例 6.8】 设 $a_1, a_2, \cdots, a_{n^2+1}$ 是 n^2+1 个不同实数的序列，证明一定可以从这个序列中选出 $n+1$ 个数的子序列 $a_{k_1}, a_{k_2}, \cdots, a_{k_{n+1}}$，使得这个子序列为递增序列或递减序列. 例如序列 15，3，20，12，30 中可以选出 3 个数的递增子序列 3，12，30 或 15，20，30.

证 假设不存在长为 $n+1$ 的递增子序列，我们来证明必存在长为 $n+1$ 的递减子序列.

对每个 $k, k = 1, 2, \cdots, n^2+1$，令 m_k 表示从 a_k 开始的递增子序列的最大长度. 由假设可知 $1 \leqslant m_k \leqslant n$. 考虑数 $m_1, m_2, \cdots, m_{n^2+1}$，这 n^2+1 个数的值只能是 $1, 2, \cdots, n$. 由定理 6.4 必有 $\left\lceil \frac{n^2+1}{n} \right\rceil = n+1$ 个 m_k 的取值相等. 设 $m_{k_1} = m_{k_2} = \cdots = m_{k_{n+1}} = l$，其中 $1 \leqslant k_1 < k_2 < \cdots < k_{n+1} \leqslant n^2+1$. 若存在某个 i 使得 $a_{k_i} < a_{k_{i+1}}$，由于 $k_i < k_{i+1}$，在从 $a_{k_{i+1}}$ 开始的最长递增子序列的前边加上 a_{k_i}，就得到了长为 $l+1$ 的从 a_{k_i} 开始的递增子序列，与 $m_{k_i} = l$ 矛盾. 因此 $a_{k_1} > a_{k_2} > \cdots > a_{k_{n+1}}$，这 $n+1$ 个数构成了长为 $n+1$ 的递减子序列. ∎

下面将鸽巢原理做进一步的推广. 先看几个简单的例子.

【例 6.9】 K_6 是 6 个顶点的完全图，用红、蓝两色涂色 K_6 的边，则或者存在一个红三角形，或者存在一个蓝三角形.

证 设 K_6 的顶点为 $v_1, v_2, \cdots, v_6$. 对于 K_6 的任何一种涂色方案，由鸽巢原理，v_1 关联的边中有 3 条同色边. 不妨设这三条边为 $\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}$.

若这三边为红色，当 v_2, v_3, v_4 之间有一条红边，比如说是 $\{v_2,$

$v_3\}$，则 $v_1v_2v_3$ 构成一个红三角形；当 v_2,v_3,v_4 之间没有红边，则 $v_2v_3v_4$ 构成一个蓝三角形.

同理可证当这三边为蓝色时命题也为真. ∎

【例 6.10】 用红、蓝两色涂色 K_9 的边，证明存在一个蓝三角形或红色的完全四边形.

证 设 K_9 的顶点为 $v_1,v_2,\cdots,v_9$. 对于 K_9 的任何一种涂色方案，必存在一个顶点连接 4 条蓝边或 6 条红边. 假若不然，每个顶点至多连接 3 条蓝边和 5 条红边. 那么蓝边总数至多为 $\left\lceil\frac{9\times3}{2}\right\rceil=13$，而红边总数至多为 $\left[\frac{9\times5}{2}\right]=22$，与 K_9 具有 $\frac{9\times8}{2}=36$ 条边矛盾. 不妨设 v_1 连接 4 条蓝边或 6 条红边.

若 v_1 连接 4 条蓝边，不妨设为 $\{v_1,v_2\},\{v_1,v_3\},\{v_1,v_4\},\{v_1,v_5\}$. 若 v_2,v_3,v_4,v_5 之间存在一条蓝边，比如说是 $\{v_2,v_3\}$，则 $v_1v_2v_3$ 构成一个蓝三角形；若 v_2,v_3,v_4,v_5 之间不存在蓝边，则这四个顶点构成一个红完全四边形.

若 v_1 连接 6 条红边，不妨设为 $\{v_1,v_2\},\{v_1,v_3\},\{v_1,v_4\},\{v_1,v_5\},\{v_1,v_6\},\{v_1,v_7\}$. 根据例 6.9，$v_2,v_3,\cdots,v_7$ 之间有一个蓝三角形或红三角形. 如果存在一个蓝三角形则命题得证；如果存在一个红三角形，则它与 v_1 构成一个红完全四边形. ∎

下面给出 Ramsey 定理的简单形式.

定理 6.5 设 p,q 是正整数，$p,q\geqslant 2$，则存在最小的正整数 $R(p,q)$，使得当 $n\geqslant R(p,q)$ 时，用红、蓝两色涂色 K_n 的边，则或者存在一个蓝色的完全 p 边形，或者存在一个红色的完全 q 边形.

证 用归纳法.

设 p 为任意正整数，$q=2$. 用红、蓝两色涂色 K_p 的边，若没有一条红边，则存在一个蓝色的完全 p 边形；若有一条红边，则构成一个完全红 2 边形，因此 $R(p,2)\leqslant p$. 同理可证 $R(2,q)\leqslant q$.

假设对一切正整数 p',q' $(p'+q'<p+q)$ 命题为真. 令 $n\geqslant$

$R(p-1,q)+R(p,q-1)$. 用红、蓝两色涂色 K_n 的边，则 v_1 或关联 $R(p-1,q)$ 条蓝边或关联 $R(p,q-1)$ 条红边. 如若不然，v_1 至多关联

$$\begin{aligned}&R(p-1,q)-1+R(p,q-1)-1\\=&R(p-1,q)+R(p,q-1)-2\end{aligned}$$

条边，与 $n \geqslant R(p-1,q)+R(p,q-1)$ 矛盾.

若 v_1 关联 $R(p-1,q)$ 条蓝边，由归纳假设这 $R(p-1,q)$ 个顶点中或含有一个蓝色的完全 $p-1$ 边形，或含有一个红色的完全 q 边形. 如为前者，则这个 $p-1$ 边形加上 v_1 构成一个蓝色的完全 p 边形，命题为真；如为后者，命题也为真.

若 v_1 关联 $R(p,q-1)$ 条红边，同理可证 K_n 中必含有一个蓝色的完全 p 边形或红色的完全 q 边形，从而证明了

$$R(p,q) \leqslant R(p-1,q)+R(p,q-1). \qquad \blacksquare$$

推论 1 $R(p,q) \leqslant \binom{p+q-2}{p-1}$ ①.

证 用归纳法.

当 $p=q=2$ 时，$R(2,2)=2$，$\binom{2+2-2}{2-1}=\binom{2}{1}=2$.

假设对一切 p'，$q'(p'+q'<p+q)$ 时命题为真，则

$$\begin{aligned}&R(p,q) \leqslant R(p-1,q)+R(p,q-1)\\ \leqslant&\binom{p-1+q-2}{p-1-1}+\binom{p+q-1-2}{p-1}\\ =&\binom{p+q-3}{p-2}+\binom{p+q-3}{p-1}=\binom{p+q-2}{p-1}. \qquad \blacksquare\end{aligned}$$

推论 2 $R(p,p) \leqslant \binom{2p-2}{P-1} \leqslant 2^{2p-2}$.

---

① $\binom{n}{m}$ 表示从 n 个元素中选取 m 个元素的组合数.

证明留作练习.

定理 6.5 说明对于给定的正整数 p,q,$R(p,q)$ 是存在的,称 $R(p,q)$ 为 **Ramsey 数**. 定理 6.5 及推论还给出了 Ramsey 数 $R(p,q)$ 的几个上界,但确定精确的 Ramsey 数的值是件相当困难的工作. 到目前为止,仅有极少数小 p,q 的 Ramsey 数被找到.

【例 6.11】 $R(3,3)=6$.

证 由例 6.9 知 $R(3,3)\leqslant 6$. 而图 6.2 中的实线代表蓝边,虚线代表红边,则这个 K_5 的涂色方案既不包含蓝三角形,也不包含红三角形. 所以 $R(3,3)>5$. 综合两方面的结果有 $R(3,3)=6$. ∎

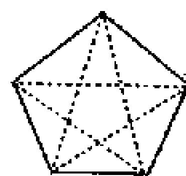


图 6.2

【例 6.12】 $R(3,4)=9$.

证 由例 6.10 知 $R(3,4)\leqslant 9$. 而图 6.3 中的实线代表蓝边,虚线代表红边,则这个 K_8 的涂色方案既不包含蓝三角形也不包含红色的完全四边形,从而 $R(3,4)>8$. 综合两方面的结果有 $R(3,4)=9$. ∎

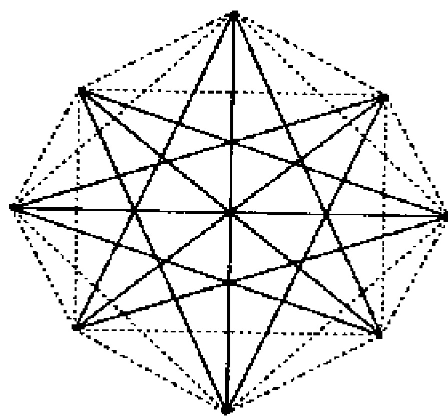


图 6.3

表 6.1(Stanislaw P. Radziszowski) 给出了到目前为止所得到的小 Ramsey 数 $R(p,q)$ 的某些精确值或上下界,其中 $3\leqslant p\leqslant 10$, $3\leqslant q\leqslant 15$. 不难证明对 Ramsey 数有下面的性质成立.

定理 6.6 设 p,q 是正整数,$p,q\geqslant 2$,则

$$R(p,q)=R(q,p).$$

证 令 $n\geqslant R(q,p)$. 对于用蓝、红两色涂色 K_n 的边的任何一种方案,将蓝边换红边,红边换蓝边,则或存在一个蓝色的完全 p 边形,或存在一个红色的完全 q 边形. 所以原来的涂色方案中必存在一个红色的完全 p 边形或一个蓝色的完全 q 边形,即 $R(q,p)\leqslant R(p,q)$. 同理可证 $R(p,q)\leqslant R(q,p)$. ∎

表 6.1

p \ q	3	4	5	6	7	8	9	10	11	12	13	14	15
3	6	9	14	18	23	28	36	40 43	46 51	51 60	60 69	66 78	73 89
4		18	25	35 41	49 62	53 85	69 116	80 151	93 191	97 238	112 291	119 349	123 417
5			43 49	58 87	76 143	95 216	317	445					
6				102 165	300	497	784	1180					
7					205 545	1035	1724	2842					
8						282 1874	3597	6116					
9							565 6680	12795					
10								798 23981					

可以使用集合论的语言来描述 Ramsey 定理.

对于给定的正整数 p,q, $p,q \geqslant 2$,存在着一个最小的正整数 $R(p,q)$,使得当 $n \geqslant R(p,q)$ 时将集合 $V=\{v_1,v_2,\cdots,v_n\}$ 的所有的 2 元子集构成的子集族划分成 E_1,E_2 两个部分,则必有 V 的 p 子集 $A=\{v_{i_1},v_{i_2},\cdots,v_{i_p}\}$ 使得 A 的所有 2 元子集都属于 E_1,或有 V 的 q 子集 $B=\{v_{j_1},v_{j_2},\cdots,v_{j_q}\}$ 使得 B 的所有 2 元子集都属于 E_2. 这里的集合 V 相当于顶点集,它的所有 2 元子集就是 K_n 的所有的边. 将所有的 2 元子集划分成 E_1 和 E_2 对应于将所有的边进行蓝和红的二着色,且 A 中顶点恰构成一个蓝色的完全 p 边形,B 中顶点恰构成一个红色的完全 q 边形.

Ramsey 进一步将这个问题推广,对任意正整数 r 考虑 V 的所有 r 元子集的划分问题,得到了关于 r 的 Ramsey 定理.

定理 6.7 对于任意给定的正整数 p,q 和 r, $p,q \geqslant r$,存在着一

个最小的正整数$R(p,q;r)$，使得当集合S的元素数$\geqslant R(p,q;r)$时，将S的r元子集族任意划分成E_1和E_2，则或者S有某个p子集A，A的所有r元子集都属于E_1，或者S有某个q子集B，B的所有r元子集都属于E_2.

证 使用多重归纳法. 首先验证

$$R(p,r;r)=p,\ R(r,q;r)=q,\ R(p,q;1)=p+q-1.$$

因为将p元集的所有r子集划分成E_1和E_2后，若$E_2=\varnothing$，则这个p元集就是集合A；若$E_2\neq\varnothing$，则属于E_2的r元子集就是集合B，所以有$R(p,r;r)\leqslant p$. 而对任何元数小于p的集合S，将S的所有r元子集都放入E_1，则S中既不存在p子集A，使得A的所有r元子集都属于E_1，也不存在r子集B使得B属于E_2，从而有$R(p,r;r)\geqslant p$. 这就证明了$R(p,r;r)=p$. 同理可证$R(r,q;r)=q$. 又根据鸽巢原理有$R(p,q;1)=p+q-1$.

假设对一切正整数p'，q'，r'(p'，$q'\geqslant r'$)存在 Ramsey 数$R(p',q';r')$，其中p',q',r'满足：

$r'=r-1$;

或 $p'=p-1,\ q'=q,\ r'=r$;

或 $p'=p,\ q'=q-1,\ r'=r$.

令

$$p_1=R(p-1,q;r),\ q_1=R(p,q-1;r),$$
$$n=R(p_1,q_1;\ r-1)+1.$$

考虑n元集S. 任取$a\in S$，令$S'=S-\{a\}$. 任给S的r元子集族的划分$\{E_1,E_2\}$，如下构造S'的$r-1$元子集族的一个划分. 设$X'=\{x_1,x_2,\cdots,x_{r-1}\}$是$S'$的一个$r-1$元子集，显然$a\notin X'$. 若$\{a\}\cup X'\in E_1$，则将$X'$放入$E'_1$；若$\{a\}\cup X'\in E_2$，则将$X'$放入$E'_2$. 易见$\{E'_1,E'_2\}$是$S'$的$r-1$元子集族的划分. 由归纳假设，下面两种情况必有一种成立：

(1) 存在S'的p_1子集A，A的所有$r-1$元子集属于E'_1；

(2) 存在 S' 的 q_1 子集 B，B 的所有 $r-1$ 元子集属于 E'_2.

若为情况(1). 由 $p_1 = R(p-1,q;r)$ 可知 A 中或者包含一个大小为 $p-1$ 的子集 X，X 的所有 r 元子集都属于 E_1；或包含一个大小为 q 的子集 Y，Y 的所有 r 元子集都属于 E_2. 如果前者成立，则 $X \cup \{a\}$ 是 S 的 p 子集，且它所有的 r 元子集都属于 E_1；若为后者，则 Y 满足要求.

若为情况(2). 由 $q_1 = R(p,q-1,r)$ 可知 B 中或者包含一个 p 子集 X，X 的所有 r 元子集都属于 E_1，或者包含一个 $q-1$ 子集 Y，Y 的所有 r 元子集都属于 E_2. 若为前者，显然命题为真；若为后者，则 $Y \cup \{a\}$ 是 S 的 q 子集，且它的所有 r 元子集都属于 E_2. ∎

推论 $R(p,q;r) \leqslant R(R(p-1,q;r),R(p,q-1;r);r-1)+1$.

在定理 6.7 中，若 $r=1$，就得到鸽巢原理(定理 6.2)；若 $r=2$，就得到 Ramsey 定理的简单形式(定理 6.5). 还可以对定理 6.7 做进一步的推广，从而得到 Ramsey 定理的一般形式.

定理 6.8 (Ramsey 定理的一般形式)

设 $r \geqslant 1, k \geqslant 1, q_i \geqslant r (i=1,2,\cdots,k)$ 是给定的正整数，则存在一个最小的正整数 $R(q_1,q_2,\cdots,q_k;r)$，使得当 $n \geqslant R(q_1,q_2,\cdots,q_k;r)$ 时将 n 元集 S 的所有 $\binom{n}{r}$ 个 r 元子集划分成 k 个子集族 $T_1,T_2,\cdots,T_k$，那么存在 S 的 q_1 元子集 A_1 且 A_1 的所有 r 元子集都属于 T_1，或者存在 S 的 q_2 元子集 A_2 且 A_2 的所有 r 元子集都属于 T_2，$\cdots$，或者存在 S 的 q_k 元子集 A_k 且 A_k 的所有 r 元子集都属于 T_k.

证 对 k 进行归纳.

$k=1$，显然有 $R(q_1;r)=q_1$.

$k=2$，根据定理 6.7，$R(q_1,q_2;r)$ 是存在的.

假设当 $k-1$ 时命题为真，令

$$n = R(q_1,R(q_2,q_3,\cdots,q_k;r);r).$$

设 S 为 n 元集，对 S 的 r 元子集做任意的 k 划分 $\{T_1,T_2,\cdots,T_k\}$. 令 T

$=T_2\cup T_3\cup\cdots\cup T_k$. 由定理 6.7 可以知道，或者在 S 中有 q_1 个元素，其所有的 r 元子集都属于 T_1，或者在 S 中有 $R(q_2,q_3,\cdots,q_k;r)$ 个元素，它们所有的 r 元子集都属于 T. 若为前者，命题显然为真. 若为后者，根据归纳假设，将 T 划分成 $k-1$ 个子集 $T_2,T_3,\cdots,T_k$ 时或有 T 的 q_2 个元素，其所有的 r 元子集都属于 T_2，或有 T 的 q_3 个元素，其所有的 r 元子集都属于 T_3，…，或有 T 的 q_k 个元素，其所有的 r 元子集都属于 T_k. 而 T 的元素就是 S 的元素. 这就证明了命题对 k 也为真. ∎

推论 $R(q_1,q_2,\cdots,q_k;r)\leqslant R(q_1,R(q_2,q_3,\cdots,q_k;r);r)$.

当 $r=2$ 时，通常省略 r，将 $R(q_1,q_2,\cdots,q_k;r)$ 记为 $R(q_1,q_2,\cdots,q_k)$. 关于一般的 Ramsey 数 $R(q_1,q_2,\cdots,q_k)$ 的值到目前为止只有一个结果，即

$$R(3,3,3)=17.$$

已知的一些上下界是：

$51\leqslant R(3,3,3,3)\leqslant 65$,

$162\leqslant R(3,3,3,3,3)\leqslant 322$,

$500\leqslant R(3,3,3,3,3,3)$,

$30\leqslant R(3,3,4)\leqslant 32$,

$45\leqslant R(3,3,5)\leqslant 59$,

$55\leqslant R(3,4,4)\leqslant 81$,

$84\leqslant R(3,3,3,4)\leqslant 159$,

$128\leqslant R(4,4,4)\leqslant 242$.

下面给出两个应用 Ramsey 定理的例子.

【例 6.13】 设 $m\geqslant 3$ 是正整数，则存在一个正整数 $N(m)$，当 $n\geqslant N(m)$ 时，若平面内的 n 个点无 3 点共线，其中总有 m 个点构成一个凸 m 边形的顶点.

为证明上述命题先证明两个引理.

引理 1 若平面内 5 个点中没有 3 点共线，则其中必有 4 个点是

一个凸 4 边形的顶点.

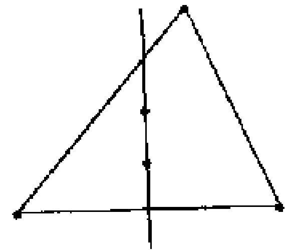


图 6.4

证 取这 5 个点的一个子集 T，使得 T 中顶点构成一个凸多边形的顶点并且剩下的点都落在 T 内. 如 $|T| = 5$，这 5 个点本身构成凸 5 边形，其中任意 4 个点都构成凸 4 边形. 若 $|T| = 4$，这 4 个点就构成凸 4 边形. 若 $|T| = 3$，如图6.4 所示. 不在 T 中的两个点确定一条直线. 根据鸽巢原理 T 中必有两点在这条直线的同侧，则这两点与直线上的两点构成一个凸 4 边形的顶点. ∎

引理 2 设平面上有 m 个点，若没有 3 点共线且任何 4 个点都是一个凸 4 边形的顶点，则这 m 个点是一个凸 m 边形的顶点.

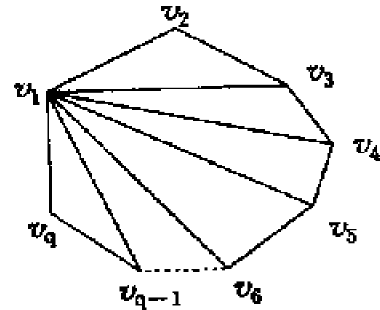


图 6.5

证 用 $\frac{m(m-1)}{2}$ 条直线将 m 个点彼此相连，假设其外周构成一个凸 q 边形，其顶点为 $v_1, v_2, \cdots, v_q$，如图 6.5. 若 $q < m$，则其余 $m - q$ 个点落入 q 边形内. 任取其中的一个点 v_x，它必落入图 6.5 中的一个三角形内，比如说 $v_1 v_r v_{r+1}$ 内，则 v_x, v_1, v_r, v_{r+1} 构成一个凹 4 边形的顶点，与已知矛盾. ∎

下面证明例 6.13 中的命题. 不妨设 $m \geqslant 4$. 令 $n \geqslant R(5, m; 4)$，S 为 n 元集. 将 S 的所有 4 元子集族进行如下划分：若它们构成一个凸 4 边形的顶点，则放入 T_2，否则放入 T_1. 根据 Ramsey 定理，或者至少有 5 个点，其一切 4 子集全是凹 4 边形的顶点；或者至少有 m 个点，其一切 4 子集全是凸 4 边形的顶点. 根据引理 1 前者是不可能成立的，根据引理 2 后者所说的 m 个点必构成一个凸 m 边形.

【例 6.14】 考虑一个通信中的噪音干扰问题. 设图 $G = \langle V, E\rangle$，其中 V 是字符表，$\forall u, v \in V$，$\{u, v\} \in E$ 当且仅当 u 和 v 在噪音干扰下传送时可能接收到相同的字符. 称 G 是通信传送的混淆图. 为了保证不同的字符在传送中不发生混淆，应该在混淆图中选择一个

顶点独立集作为通信的字符集. 设 $\beta_0(G)$ 是 G 的点独立数，则 $\beta_0(G)$ 是不会发生混淆的最大字符集的字符个数.

下面考虑字符串的传送问题. 先定义图 G 和 H 的正规积.

定义 6.1　设 $G = \langle V_1, E_1 \rangle$, $H = \langle V_2, E_2 \rangle$ 是图. 令 $V = V_1 \times V_2$, $\forall \langle a,b \rangle, \langle c,d \rangle \in V_1 \times V_2$, $\{\langle a,b \rangle, \langle c,d \rangle\} \in E$ 当且仅当下述条件中至少成立一条.

(1) $\{a,c\} \in E_1$ 且 $\{b,d\} \in E_2$;

(2) $a = c$ 且 $\{b,d\} \in E_2$;

(3) $b = d$ 且 $\{a,c\} \in E_1$.

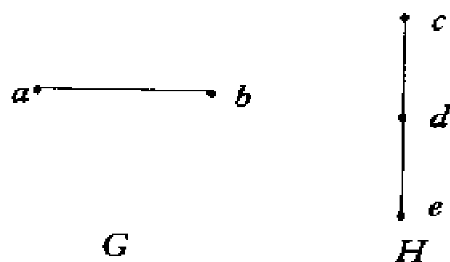


图 6.6

称图 $G' = \langle V, E \rangle$ 是 G 与 H 的**正规积**，记作 $G \cdot H$.

例如 G, H 如图 6.6 所示，则

$V = V_1 \times V_2 = \{\langle a,c \rangle, \langle a,d \rangle, \langle a,e \rangle, \langle b,c \rangle, \langle b,d \rangle, \langle b,e \rangle\}$，且积图 $G \cdot H = \langle V, E \rangle$ 如图 6.7 所示. 若将 G, H 的顶点看作字符，则积图的顶点恰为 G 中字符连结 H 中的字符所构成的长为 2 的字符串.

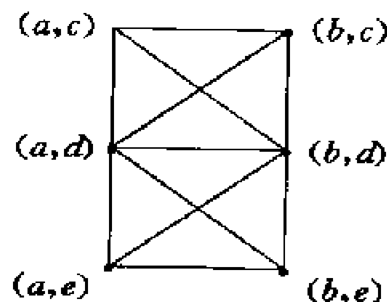


图 6.7

设 xy 和 uv 是字符集上长为 2 的字符串，若规定：

xy 与 uv 混淆当且仅当以下条件成立其一.

(1) x 与 u 混淆且 y 与 v 混淆；

(2) $x = u$ 且 y 与 v 混淆；

(3) x 与 u 混淆且 $y = v$.

那么不难看出字符串的混淆图恰为字符混淆图 G 的正规积 $G \cdot G$. 可以证明正规积的点独立数 $\beta_0(G \cdot H)$ 与图 G, H 的点独立数 $\beta_0(G)$ 和 $\beta_0(H)$ 之间存在下面的关系.

定理 6.9　$\beta_0(G \cdot H) \leqslant R(\beta_0(G) + 1, \beta_0(H) + 1) - 1$.

证　假设 $\beta_0(G \cdot H) \geqslant R(\beta_0(G) + 1, \beta_0(H) + 1) = n$. 令 A 是

$G \cdot G$ 中一个大小为 $R(\beta_0(G)+1,\beta_0(H)+1)$ 的点独立集. 对任意 $\langle a,b\rangle,\langle c,d\rangle \in A$,则只有下面两种情况:

(1) $a \neq c$ 且 $\{a,c\} \notin E_1$,其中 E_1 是 G 的边集;

(2) $a=c$ 或 $\{a,c\} \in E_1$,但 $b \neq d$ 且 $\{b,d\} \notin E_2$,其中 E_2 是 H 的边集.

用蓝、红两色涂色由 A 中顶点构成的完全 n 边形的边, 若 $\langle a,b\rangle$, $\langle c,d\rangle$ 满足(1),则涂成蓝色;若满足(2),则涂成红色. 根据 Ramsey 定理,K_n 中或者存在一个蓝色的完全 $\beta_0(G)+1$ 边形,或者存在一个红色的完全 $\beta_0(H)+1$ 边形. 若为前者,令

$$A_1 = \{x \mid \langle x,y\rangle \text{ 是蓝色完全 } \beta_0(G)+1 \text{ 边形的顶点}\},$$

则 A_1 是 G 中大小为 $\beta_0(G)+1$ 的点独立集,与 G 中点独立数为 $\beta_0(G)$ 矛盾. 若为后者,同理可证与 H 中点独立数是 $\beta_0(H)$ 矛盾. ∎

为了得到比较大的不混淆的代码集,可以利用不混淆的字符集来构成字符串. 若字符表中有 5 个字符,其中不混淆的字符有 3 个. 当构造长为 2 的字符串时,不混淆的长为 2 的串至多为

$$R(3+1,3+1)-1 = R(4,4)-1 = 17$$

个.

§6.2 相异代表系

我们先回顾一下图论中的 Hall 定理.

定理 6.10 设 $G=\langle X,Y,E\rangle$ 是二部图,$\forall a \in X$ 令

$$\Gamma(a) = \{u \mid u \in Y \wedge \{a,u\} \in E\}.$$

$\forall A \subseteq X$,令 $\Gamma(A) = \bigcup_{a\in A} \Gamma(a)$,则在 G 中存在着从 X 到 Y 的完美匹配的充要条件是对任何 $A \subseteq X$ 有 $|\Gamma(A)| \geqslant |A|$.

【例 6.15】 考虑如图 6.8 中的 5×3 数组. 从数字 $1,2,\cdots,7$ 中选择 5 个数字构成一个新的列加到原来的数组上而得到一个 5×4 数组. 如果要求这个新数组的每列的元素彼此不等,且每

3	7	1
2	6	5
4	3	6
1	2	3
5	4	2

图 6.8

行的元素也彼此不等，问能否构成这样的新数组？为什么？

解 令 $X=\{1,2,3,4,5\}$，$Y=\{1,2,\cdots,7\}$. $\forall x\in X$，$y\in Y$，$\{x,y\}\in E\Leftrightarrow$ 在 5×3 数组中 y 不在行 x 出现，则 $G=\langle X,Y,E\rangle$ 是一个二部图，如图6.9所示. 如果 G 存在完美匹配，$\{x,y\}$ 是一条匹配边，则将 y 加到原数组的第 x 行上，这样得到的 5×4 数组满足要求. 下面验证 Hall 定理的条件.

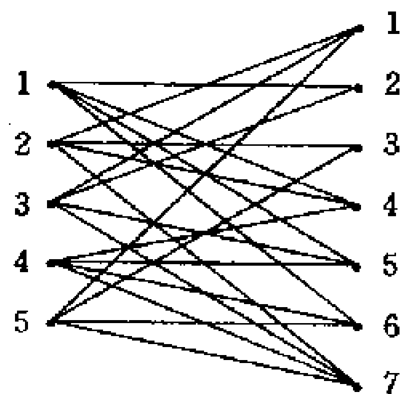


图 6.9

$\forall x\in X$，有 $|\Gamma(x)|=4$，因此对 X 的任何子集 A，若 $|A|\leqslant 4$，必有 $|\Gamma(A)|\geqslant|A|$. 而 X 的 5 元子集只有一个，就是 X 自身. 而 $|\Gamma(X)|=7\geqslant 5=|X|$. G 满足 Hall 定理条件，因此可以构成满足题设条件的 5×4 数组.

下面考虑子集族的相异代表系问题.

定义 6.2 设 S 为有穷集，$A_0,A_1,\cdots,A_{n-1}$ 是 S 的不同的子集. 一个关于 $A_0,A_1,\cdots,A_{n-1}$ 的相异代表系是由不同元素构成的有序 n 元组 $\langle a_0,a_1,\cdots,a_{n-1}\rangle$，使得 $a_i\in A_i$，$0\leqslant i\leqslant n-1$.

【例 6.16】 $S=\{x_0,x_1,\cdots,x_5\}$，问对于以下 S 的子集族是否存在相异代表系？

(1) $A_0=\{x_0\}$，$A_1=\{x_0,x_1\}$，$A_2=\{x_1\}$；

(2) $A_0=\{x_0,x_1\}$，$A_1=\{x_2,x_3\}$，$A_2=\{x_0,x_2\}$.

解 (1) 不存在相异代表系. 因为 A_0 中只能选 x_0，因此 A_1 中只能选 x_1，而 A_2 中既不能选 x_0，也不能选 x_1，无元素可选.

(2) 存在相异代表系，例如 $\langle x_0,x_3,x_2\rangle$，$\langle x_1,x_2,x_0\rangle$，$\langle x_1,x_3,x_0\rangle$，$\langle x_1,x_3,x_2\rangle$ 等都是关于 A_0,A_1,A_2 的相异代表系.

上述的问题是一个典型的组合存在性问题. 可以使用集合论的方法来描述这个问题，这就是相异代表系问题. 也可以使用图论的方法来描述这个问题，那就是二部图的完美匹配问题.

考虑二部图 $G=\langle X,Y,E\rangle$，设 $X=\{x_0,x_1,\cdots,x_{n-1}\}$，$Y=\{y_0,y_1,\cdots,y_{m-1}\}$. 对于任意的 $x_i\in X$，$\Gamma(x_i)\subseteq Y$，因此 $\Gamma(x_0),\Gamma(x_1),\cdots,\Gamma(x_{n-1})$ 构成 Y 的子集族. 易见 G 中存在完美匹配

$$M=\{\{x_j,\ y_{i_j}\}\mid j=0,1,\cdots,n-1\}$$

当且仅当 $\langle y_{i_0},y_{i_1},\cdots,y_{i_{n-1}}\rangle$ 是子集族 $\Gamma(x_0),\Gamma(x_1),\cdots,\Gamma(x_{n-1})$ 的一个相异代表系. 二部图 G 的完美匹配问题转化成了集合族的相异代表系问题. 反之，给定集合族 $A_0,A_1,\cdots,A_{n-1}$，如下构造二部图 $G=\langle X,Y,E\rangle$. 任取 n 元集 $X=\{x_0,x_1,\cdots,x_{n-1}\}$，令 $Y=A_0\cup A_1\cup\cdots\cup A_{n-1}$. 对任意的 $x_j\in X$，$y\in A_j$，边 $\{x_j,y\}\in E$，$j=0,1,\cdots,n-1$. 易见 $A_0,A_1,\cdots,A_{n-1}$ 存在相异代表系 $\langle y_{i_0},y_{i_1},\cdots,y_{i_{n-1}}\rangle$ 当且仅当

$$\{\{x_j,y_{i_j}\}\mid j=0,1,\cdots,n-1\}$$

是 G 的完美匹配. 根据 Hall 定理可以得到下面的定理：

定理 6.11　设 S 是有穷集，$A_0,A_1,\cdots,A_{n-1}$ 是 S 的子集族. $A_0,A_1,\cdots,A_{n-1}$ 存在相异代表系当且仅当对所有的 k，$1\leqslant k\leqslant n$，该子集族的任意 k 个子集的并都至少含有 k 个元素.

在某些情况下对于子集族 $A_0,A_1,\cdots,A_{n-1}$ 并不存在相异代表系，但对其中的一部分子集可以存在相异代表系. 我们希望确定具有相异代表系的子集族所含子集的最多个数. 例如子集族 $A_0=\{1,4\}$，$A_1=\{1,2\}$，$A_2=\{2,4\}$，$A_3=\{1,3,4,5\}$，$A_4=\{1,4\}$. 由 $|A_0\cup A_1\cup A_2\cup A_4|=3$ 可知 A_0,A_1,A_2,A_3,A_4 并不具有相异代表系，但 A_0,A_1,A_2,A_3 满足定理 6.11 条件，具有相异代表系. 例如 $\langle 1,2,4,3\rangle$，$\langle 1,2,4,5\rangle$，$\langle 4,1,2,3\rangle$，$\langle 4,1,2,5\rangle$ 等都是相异代表系，因此具有相异代表系的子集族至多含有 4 个子集.

定理 6.12　设 S 是有穷集，$A_0,A_1,\cdots,A_{n-1}$ 是 S 的子集族. r 是正整数，$r\leqslant n$. 则在 $A_0,A_1,\cdots,A_{n-1}$ 中含有 r 个子集构成具有相异代表系的子集族当且仅当对所有的 k，$1\leqslant k\leqslant n$，$A_0,A_1,\cdots,A_{n-1}$ 中任意 k 个子集的并都至少含有 $k-(n-r)$ 个元素.

证 令 B 是 $n-r$ 个元素的集合，且 $\forall A_i, i=0,1,\cdots,n-1$，满足 $A_i \cap B = \varnothing$. 考虑集合族 $A_0 \cup B, A_1 \cup B, \cdots, A_{n-1} \cup B$. 下面证明 $A_0, A_1, \cdots, A_{n-1}$ 中有 r 个子集具有一个相异代表系当且仅当 $A_0 \cup B, A_1 \cup B, \cdots, A_{n-1} \cup B$ 具有一个相异代表系.

设 $A_0, A_1, \cdots, A_{n-1}$ 中有 r 个子集具有相异代表系，不妨设这些子集是 $A_0, A_1, \cdots, A_{r-1}$，且相异代表系是 $\langle a_0, a_1, \cdots, a_{r-1}\rangle$. 令 $B=\{b_1, b_2, \cdots, b_{n-r}\}$，则 $\langle a_0, a_1, \cdots, a_{r-1}, b_1, b_2, \cdots, b_{n-r}\rangle$ 是 $A_0 \cup B, A_1 \cup B, \cdots, A_{n-1} \cup B$ 的相异代表系. 反之，设 $\langle x_0, x_1, \cdots, x_{n-1}\rangle$ 是 $A_0 \cup B, A_1 \cup B, \cdots, A_{n-1} \cup B$ 的相异代表系. 因为 $|B|=n-r$，所以 $x_0, x_1, \cdots, x_{n-1}$ 中至少有 r 个元素属于 $A_0, A_1, \cdots, A_{n-1}$ 中的 r 个子集，即有 $x_{i_1} \in A_{i_1}$，$x_{i_2} \in A_{i_2}, \cdots, x_{i_r} \in A_{i_r}$. 这就证明 $\langle x_{i_1}, x_{i_2}, \cdots, x_{i_r}\rangle$ 是 $A_{i_1}, A_{i_2}, \cdots, A_{i_r}$ 的相异代表系.

根据定理 6.11，$A_0 \cup B, A_1 \cup B, \cdots, A_{n-1} \cup B$ 具有相异代表系当且仅当对所有的 $k, 1 \leqslant k \leqslant n$，这 n 个集合中的任意 k 个集合的并都至少含有 k 个元素. 设 $A_{i_1}, A_{i_2}, \cdots, A_{i_k}$ 是 $A_0, A_1, \cdots, A_{n-1}$ 中的任意 k 个集合，则 $A_{i_1} \cup B, A_{i_2} \cup B, \cdots, A_{i_k} \cup B$ 是 $A_0 \cup B, A_1 \cup B, \cdots, A_{n-1} \cup B$ 中的 k 个集合，而

$$
\begin{aligned}
& |A_{i_1} \cup B \cup A_{i_2} \cup B \cup \cdots \cup A_{i_k} \cup B| \geqslant k \\
\Leftrightarrow\ & |A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}| \geqslant k - |B| \\
\Leftrightarrow\ & |A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}| \geqslant k - (n-r). \qquad \blacksquare
\end{aligned}
$$

如果在定理 6.12 中，令 $r=n$，就得到定理 6.11. 定理 6.11 是定理 6.12 的特例.

下面考虑一个 $(0-1)$ 矩阵的问题，先给出有关的概念.

定义 6.3 设 $M=(a_{ij})$ 是 k 阶矩阵，其中 $a_{ij}=0$ 或 1. m, n 是正整数，n 为行数，m 为列数且使得这 n 行和 m 列包含了 M 中所有的 1. 称这 n 行和 m 列为 M 的一个**覆盖**，$n+m$ 为**覆盖数**.

定义 6.4 设 $M=(a_{ij})$ 是 k 阶 $(0-1)$ 矩阵，a_{ij}, a_{st} 为 M 中的

两个 1，若 $i \neq t,\ j \neq s$，则称这两个 1 是**相离**的.

定理 6.13　设 $M = (a_{ij})$ 为 k 阶 $(0-1)$ 矩阵，则 M 中含相离的 1 的最多个数等于 M 的最小覆盖数.

证　令 m_1 是 M 的最小覆盖数，m_2 是 M 中所含相离的 1 的最多个数，显然 $m_1 \geqslant m_2$.

设 M 的最小覆盖由 r 行 s 列构成，$m_1 = r + s$，不妨设是 M 的前 r 行和前 s 列. 定义集合族

$$A_i = \{j \mid j > s \wedge a_{ij} = 1\},\ i = 1,2,\cdots,r.$$

若存在 k 个集合 $(1 \leqslant k \leqslant r)$ 其元素总数小于 k，则可以用 $k-1$ 个列代替这 k 个行，从而得到一个覆盖数小于 $r+s$ 的覆盖，与 $r+s$ 为最小覆盖数矛盾. 所以子集族 $A_1, A_2, \cdots, A_r$ 满足定理 6.11 的条件，故存在相异代表系. 即在矩阵的前 r 行上存在 r 个 1，其中任何两个 1 都不在同一行上，也不在前 s 列上. 同理可证在前 s 列上也存在 s 个 1，没有两个 1 在同一列上，也不在前 r 行上. 这就推出 $m_2 \geqslant r + s = m_1$.

综合以上的结果有 $m_1 = m_2$. ∎

定义 6.5　设 P 是 $n \times n$ 的 $(0-1)$ 矩阵，如果

$$PP^T = E_n,$$

则称 P 为**置换矩阵**，其中 P^T 为 P 的转置，E_n 为 n 阶单位矩阵.

定理 6.14　设 P 是 $n \times n$ 的 $(0-1)$ 矩阵，则 P 为置换矩阵的充要条件是每行每列恰有一个 1.

证　若 P 为置换矩阵当且仅当

$$\sum_{1 \leqslant k \leqslant n} p_{ik} p_{jk} = \begin{cases} 1, & \text{若 } i = j, \\ 0, & \text{否则}. \end{cases}$$

由 $\sum\limits_{1 \leqslant k \leqslant n} p_{ik} p_{jk} = 1\ (i = j)$ 可知对于给定的 i，恰有一个 $p_{ij} = 1$，即 P 的每行恰含一个 1. 又由 $\sum\limits_{1 \leqslant k \leqslant n} p_{ik} p_{jk} = 0\ (i \neq j)$ 可知 P 的每列至多含一个 1. 因此 P 的每行每列恰含一个 1.

反之，若 P 的每行每列恰含一个 1，对于 $i = 1,2,\cdots,n$，设第 i 行

的第 j_i 个元素 $p_{ij_i}=1$，则 $j_1,j_2,\cdots,j_n$ 为 $\{1,2,\cdots,n\}$ 的一个排列，所以有 $\sum\limits_{1\leqslant k\leqslant n} p_{ik}p_{jk}=\begin{cases}1, & 当\ i=j,\\ 0, & 否则.\end{cases}$ ∎

定理6.15 设 $M_n(N)$ 是自然数集 N 上所有 n 阶矩阵的集合，$M=(a_{ij})\in M_n(N)$. 若

$$\sum_j a_{ij}=\sum_i a_{ij}=l,\quad l\in Z^+,$$

则 M 可以表成 l 个 $(0-1)$ 置换矩阵之和.

证 对 l 进行归纳.

$l=1$. 由于 M 的每行恰有一个 1，每列也恰有一个 1. 根据定理 6.14，M 本身就是一个置换矩阵.

假设对 $l=t$ 命题为真. 考虑 $l=t+1$ 的情况. 对于 $1\leqslant i\leqslant n$，令 $A_i=\{j\mid a_{ij}>0\}$. 对任意的 $k\in Z^+,k\leqslant n$，任取其中的 k 个集合 $A_{s_1},A_{s_1},\cdots,A_{s_k}$，令 $S=\{s_1,s_2,\cdots,s_k\}$，则这 k 行非零元素之和为

$$\sum_{i\in S}\sum_{j=1}^{n}a_{ij}=k(t+1).$$

由于每列元素之和为 $t+1$，这 k 行的非零元素至少分布到 k 列中，所以有

$$|A_{s_1}\cup A_{s_2}\cup\cdots\cup A_{s_k}|\geqslant k.$$

这说明集合族 $A_1,A_2,\cdots,A_n$ 满足定理 6.11 的相异性条件，所以存在一个相异代表系 $\langle p_1,p_2,\cdots,p_n\rangle$，$p_j\in A_j$，$j=1,2,\cdots,n$. 令第一行 p_1 列的元素为 1，第二行 p_2 列的元素为 1，…，第 n 行 p_n 列的元素为 1，剩下的元素全为 0，从而得到一个对应于这个相异代表系的 $(0-1)$ 置换矩阵 P_1. 令 $M_1=M-P_1$，则 M_1 为自然数集 N 上的 n 阶矩阵，且 $\sum\limits_j a_{ij}=\sum\limits_i a_{ij}=l-1=t$，$M_1=(a_{ij})_{n\times n}$. 由归纳假设 M_1 可以表为 t 个 $(0-1)$ 置换矩阵之和，即

$$M_1=P_2+P_3+\cdots+P_{t+1},$$

其中 $P_2,P_3,\cdots,P_{t+1}$ 为置换矩阵，从而得到

$$M = P_1 + M_1 = P_1 + P_2 + \cdots + P_{s+1}.$$ ∎

【例 6.17】 设

$$M = \begin{bmatrix} 0 & 2 & 0 & 4 \\ 1 & 3 & 2 & 0 \\ 2 & 1 & 1 & 2 \\ 3 & 0 & 3 & 0 \end{bmatrix},$$

试给出 M 的置换矩阵表示式.

解 令 $A_{11} = \{2,4\}$, $A_{12} = \{1,2,3\}$, $A_{13} = \{1,2,3,4\}$, $A_{14} = \{1,3\}$. $A_{11}, A_{12}, A_{13}, A_{14}$ 的一个相异代表系是 $X_1 = \langle 2,3,4,1 \rangle$,对应于 X_1 的置换矩阵是

$$P_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

令 $M_1 = M - P_1 = \begin{bmatrix} 0 & 1 & 0 & 4 \\ 1 & 3 & 1 & 0 \\ 2 & 1 & 1 & 1 \\ 2 & 0 & 3 & 0 \end{bmatrix}$,得到 $A_{21} = \{2,4\}$, $A_{22} = \{1,2,3\}$, $A_{23} = \{1,2,3,4\}$, $A_{24} = \{1,3\}$. $A_{21}, A_{22}, A_{23}, A_{24}$ 的一个相异代表系是 $X_2 = \langle 2,3,4,1 \rangle$. 对应于 X_2 的置换矩阵是

$$P_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

再令 $M_2 = M_1 - P_2$, 得到 $M_2 = \begin{bmatrix} 0 & 0 & 0 & 4 \\ 1 & 3 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 3 & 0 \end{bmatrix}$. 从而 $A_{31} = \{4\}$, $A_{32} = \{1,2\}$, $A_{33} = \{1,2,3\}$, $A_{34} = \{1,3\}$. $A_{31}, A_{32}, A_{33}, A_{34}$ 的相异代表系是 $X_3 = \langle 4,1,2,3 \rangle$. 对应于 X_3 的置换矩阵是

$$P_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

令 $M_3 = M_2 - P_3 = \begin{bmatrix} 0 & 0 & 0 & 3 \\ 0 & 3 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 \end{bmatrix}$,因此 $A_{41} = \{4\}$, $A_{42} = \{2\}$, $A_{43} = \{1,3\}$, $A_{44} = \{1,3\}$. $A_{41},A_{42},A_{43},A_{44}$ 的相异代表系是 $X_4 = \langle 4,2,1,3\rangle$. 对应于 X_4 的置换矩阵

$$P_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

令 $M_4 = M_3 - P_4 = \begin{bmatrix} 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$. 因此 $A_{51} = \{4\}$, $A_{52} = \{2\}$, $A_{53} = \{1,3\}$, $A_{54} = \{1,3\}$. $A_{51},A_{52},A_{53},A_{54}$ 的相异代表系是 $X_5 = \langle 4,2,1,3\rangle$,对应于 X_5 的置换矩阵是

$$P_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

令 $M_5 = M_4 - P_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. 分解到此终止,最后得到

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} +$$
$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

关于偏序集的分解定理已在集合论部分作了介绍,这里不再重复. 有趣的是这个定理和 Hall 定理有着密切的关系,可以使用这个定理给出一个 Hall 定理的证明.

设 $G=\langle X,Y,E\rangle$ 是二部图,其中 $|X|=n$, $|Y|=n'\geqslant n$. 定义 $X\cup Y$ 上的关系 R, $\forall x\forall y(x\in X$ 且 $y\in Y)$,

$$xRy\Leftrightarrow\{x,y\}\in E,$$

则 $R\cup I_{X\cup Y}$ 是 $X\cup Y$ 上的偏序,其中 $I_{X\cup Y}$ 为 $X\cup Y$ 上的恒等关系. 假定偏序集上最长反链的长度是 s,设这个反链为 $\{x_1,x_2,\cdots,x_l,\ y_1,y_2,\cdots,y_k\}$, $l+k=s$. 由于

$$\Gamma(\{x_1,\cdots,x_l\})\subseteq Y-\{y_1,y_2,\cdots,y_k\},$$

所以 $l\leqslant n'-k$. 即 $s=l+k\leqslant n'$. 根据偏序集的分解定理,偏序集可以分解为 s 条不交的链. 设 G 中最大匹配数为 m. 每条匹配边都对应于一条链, X 中还剩下 $n-m$ 个元素, Y 中剩下 $n'-m$ 个元素,总的链数为

$$m+n-m+n'-m=s\leqslant n'.$$

因此 $n+n'-m\leqslant n'$,从而有 $n\leqslant m$,于是存在完美匹配.

必要性是显然的. Hall 定理得证.

习　题　六

1. (1) 在边长为 1 的等边三角形内任意放 10 个点,证明一定存在两个点,其距离不大于 1/3;

(2) 确定正整数 m_n 的值,使得在边长为 1 的等边三角形内任意放 m_n 个点,其中必有两点的距离不大于 $1/n$.

2. 证明一个有理数的十进小数展开式自某一位后必是循环的.

3. 证明对任意的正整数 N 存在着 N 的一个倍数,使得它仅由数字 0 和 7 组成(例如 $N=3$,我们有 $3\times 259=777$; $N=4$,有 $4\times 1925=7700$; $N=5$,有 $5\times 14=70,\cdots$).

4. (1) 证明在任意选取的 $n+1$ 个正整数中存在着两个正整数,其差能被 n 整除;

(2) 证明在任意选取的 $n+2$ 个正整数中存在着两个正整数,其差能被 $2n$ 整除或者其和能被 $2n$ 整除.

5. 某学生有 37 天的时间准备考试. 根据她过去的经验至多需要复习 60 小时,但每天至少要复习 1 小时. 证明无论怎样安排都存在着连续的若干天,使得她在这些天内恰好复习了 13 小时.

6. 证明任何一组人中都存在两个人,他们在组内认识的人数恰好相等.

7. (1) 证明每年中至少有一个 13 日是星期五.

(2) 证明每年中至多有三个 13 日是星期五.

8. 证明将 m 个球放入 n 个盒子,至少有一个盒子里有 $\left[\frac{m-1}{n}\right]+1$ 个球,但可能有一种放法使所有的盒了里不含有多于 $\left[\frac{m-1}{n}\right]+1$ 个球.

9. 将 m 个球放入 n 个盒子里,证明若 $m<\frac{n(n-1)}{2}$,则至少有两个盒子里有相同数目的球.

10. 把一个圆盘分成 36 个相等的扇形,然后把 1,2,…,36 这些数任意填入 36 个扇形中. 证明存在三个连接的扇形,其中的数字之和至少是 56.

11. 证明定理 6.5 的推论 2.

12. 不使用例 6.10 的结果证明对任意 10 个顶点的图 G 或者在 G 中存在大小为 3 的团,或者在 G 的补图 $\overline{G}$ 中存在大小为 4 的点独立集.

13. 证明 $R(r,r,q;r)=q$.

14. 设 $q_1,q_2,\cdots,q_n,r$ 为正整数,$q_i\geqslant r,i=1,2,\cdots,n$. 令 $Q=\max\{q_1,q_2,\cdots,q_n\}$,证明

$$R(Q,Q,\cdots,Q;r)\geqslant R(q_1,q_2,\cdots,q_n;r).$$

15. 证明 $R(3,5)=14$.

16. 有四个文件 A,B,C,D,每个文件有一个 3 位数的代码如下:

A: 123, B: 303, C:111, D:222.

问能否对每个文件从它的代码中选取一位数字,使得这四个文件用一位代码来识别?

17. 确定下列集合族的所有的相异代表系.

(1) $A_1=\{1,2\}$, $A_2=\{2,3\}$, $A_3=\{3,4\}$, $A_4=\{4,5\}$, $A_5=\{5,1\}$;

(2) $A_1=\{1,2\}$, $A_2=\{2,3\}$, …, $A_n=\{n,1\}$.

18. 有四个码字: *abcd*, *cde*, *ab*, *ce* 需要存入计算机,我们希望对每个码字从其字母中选择一个字母作为代表存入. 如果要求每个码字存入的字母互不相

定理 7.1　设 n,r 是正整数，且 $n \geqslant r$，则

$$p(n,r) = n(n-1)\cdots(n-r+1).$$

证　从 n 元集中选取第一个元素有 n 种方法；在选好了第一元素后第二个元素只能取自剩下的 $n-1$ 个元素，选法有 $n-1$ 种；类似地第三个元素有 $n-2$ 种选法；…；最后一个元素，也就是第 r 个元素有 $n-r+1$ 种选法. 根据乘法法则，选法总数为 $n(n-1)\cdots(n-r+1)$. ∎

我们使用 $n!$ 来表示 $n(n-1)\cdots 2\cdot 1$ 且规定 $0!=1$ 和 $P(n,0)=1$，则有

$$P(n,r)=\begin{cases}\dfrac{n!}{(n-r)!}, & n \geqslant r \geqslant 0,\\ 0, & n<r.\end{cases}$$

【例 7.9】　排列 26 个字母，使得在 a 和 b 之间正好有 7 个字母，问有多少种排法？

解　以 a 排头、b 排尾、中间恰含 7 个字母的排列有 $P(24,7)$ 种. 同理以 b 排头、a 排尾、中间恰含 7 个字母的排列也有 $P(24,7)$ 种. 由加法法则以 a,b 为两端的 9 个字母的排列有 $2P(24,7)$ 种. 把一个这样的排列看成一个整体再与剩下的 17 个字母进行全排列就得到所求的排列. 全排列方法是 $18!$ 种，根据乘法法则，所求的排列数

$$N = 2P(24,7) \times 18! = 36 \times 24!.$$

以上讨论的排列确切地说应该叫做线形排列. 如果我们把集合的元素排成一个环，那么排列数将会减少，因为对于两个环排列，如果其中的一个通过旋转可以变成另一个，则认为它们是同样的环排列.

定理 7.2　一个 n 元集 S 的环形 r- 排列数是

$$\frac{P(n,r)}{r} = \frac{n!}{r(n-r)!},$$

如果 $r=n$，则 S 的环排列数是 $(n-1)!$.

第七章　基本的计数公式

本章以加法法则和乘法法则为基础，讨论了选取问题的一些基本计数公式和组合恒等式.

§7.1　两个计数原则

有两个基本的计数原则：加法法则和乘法法则.

加法法则　设事件 A 有 p 种产生的方式，事件 B 有 q 种产生的方式，若事件 A 与 B 产生的方式不重叠，则事件"A 或 B"有 $p+q$ 种产生的方式.

【例7.1】　从 A 城到 B 城乘飞机、火车、轮船各有1种方式，乘汽车有3种方式，则从 A 城到 B 城共有 $1+1+1+3=6$ 种方式.

【例7.2】　7个学生中有5人学习英语，4人学习日语，1人不学英语也不学日语，则这些学生中学习英语或日语的学生不是 $5+4=9$ 人，而是6人. 这里不能使用加法法则，因为有3人同时学习英语和日语. 学英语和学日语的人有重叠，破坏了加法法则的使用条件.

乘法法则　设事件 A 有 p 种产生的方式，事件 B 有 q 种产生的方式. 若事件 A 与事件 B 的产生是彼此独立的，则事件"A 与 B"有 pq 种产生的方式.

【例7.3】　从 A 城到 B 城有3种方式，从 B 城到 C 城有2种方式，则从 A 城经过 B 城到 C 城有 $3\times 2=6$ 种方式.

【例7.4】　从4张不同的明信片中选取2张分别寄给2个朋友，则有 $4\times 3=12$ 种不同的寄法，而不是 $4\times 4=16$ 种不同的寄法. 尽管每个朋友可能会得到任何一张明信片，但当其中的一个人选定一张明信片后，另一个独立的选法只有3种，而不是4种.

加法法则和乘法法则可以推广到有限个事件的情况，即：

加法法则　设事件 $A_1,A_2,\cdots,A_n$ 分别有 $p_1,p_2,\cdots,p_n$ 种产生的

对选好的 r 个元素进行排列，排列数为 $r!$. 根据乘法法则 n 元集的 r- 排列数为 $C(n,r)\cdot r!$，即 $P(n,r)=C(n,r)\cdot r!$，定理得证. ∎

易见当 $r>n$ 时有 $C(n,r)=0$. 当 $r=0$ 时，规定 $C(n,r)=1$. 那么有

$$C(n,r)=\begin{cases}\dfrac{n!}{r!(n-r)!}, & n\geqslant r\geqslant 0,\\ 0, & n<r.\end{cases}$$

推论 设 $n,r\in N$，对一切 $n\geqslant r$ 有

$$C(n,r)=C(n,n-r).$$

证 $C(n,r)=\dfrac{n!}{r!(n-r)!}=\dfrac{n!}{[n-(n-r)]!(n-r)!}$

$=C(n,n-r).$ ∎

【例 7.11】 从 $1,2,\cdots,300$ 中任取三个数使得它们的和能被 3 整除，问有多少种方法？

解 把 $1,2,\cdots,300$ 分成 A,B,C 三组：

$A=\{x\mid(x)\text{mod}3=1\}$，

$B=\{x\mid(x)\text{mod}3=2\}$，

$C=\{x\mid(x)\text{mod}3=0\}$.

设所取的数为 i,j,k. 那么这种选取是无序的，且满足 $(i+j+k)\text{mod}3=0$. 将选法分成两类：

i,j,k 都取自同一组，方法数 $N_1=3C(100,3)$.

i,j,k 分别取自 A,B,C，方法数 $N_2=[C(100,1)]^3$. 由加法法则可得取法总数为

$$N=3C(100,3)+[C(100,1)]^3=1485100.$$

【例 7.12】 证明 $C(2n,2)=2C(n,2)+n^2$.

证 采用组合分析的方法. 等式左边表示从 $2n$ 个不同的球中选取 2 个球的方法数. 我们把这 $2n$ 个球平均分成 A,B 两组，选球的方法有两类：

的数字.对于某四个数字,如果选择的次序不同就会得到不同的四位数.所以这两个问题都是从某个集合有序地选取若干个元素的问题,我们称之为**排列**问题.问题(1)和(2)的不同点仅在于(1)中的选取不允许重复而(2)中的选取允许重复.

【例 7.8】 (1)从 5 种不同的球中每次取 3 个不同的球,问有多少种取法?

(2)从 5 种不同的球中(每种球的个数至少为 3 个)每次取 3 个球,问有多少种取法?

这两个问题的取法仅与选取的是哪几个球有关而与球取出的次序无关.它们都是从某个集合中无序地选取若干个元素的问题,我们称之为**组合**问题.这两个问题的区别仅在于问题(1)的选取不允许重复,而问题(2)的选取允许重复.

为了处理允许重复的有序或无序选取问题先给出多重集的定义.

定义 7.1 元素可以多次出现的集合称为**多重集**,元素 a_i 出现的次数叫做该元素的**重复数**,记作 n_i,$n_i = 0,1,\cdots,\infty$.含有 k 种元素的多种集 S 可记作 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$.

例如 $S_1 = \{2 \cdot a,\ 4 \cdot b,\ 5 \cdot c\}$,$S_2 = \{\infty \cdot a,\ \infty \cdot b,\ \infty \cdot c\}$ 都是多重集.

根据选取是否有序与是否可重复而将选取划分成以下四类:

集合的排列　　　　有序的不允许重复的选取;

集合的组合　　　　无序的不允许重复的选取;

多重集的排列　　　有序的允许重复的选取;

多重集的组合　　　无序的允许重复的选取.

下面给出关于这四类选取问题的计数公式.

定义 7.2 从 n 元集 S 中有序选取的 r 个元素叫做 S 的一个 **r-排列**,不同排列的总数记作 $P(n,r)$.如果 $r = n$,则称这个排列为 S 的**全排列**,简称为 S 的排列.

同，给出所有可能的存入方法.

19. 令 $A_i=\{1,2,\cdots,n\}-\{i\}$，$i=1,2,\cdots,n$. 证明集合族 $A_1,A_2,\cdots,A_n$ 存在相异代表系.

20. 设 $M\in M_5(N)$，且

$$M=\begin{pmatrix}2&1&0&1&2\\1&3&1&0&1\\0&0&3&2&1\\1&1&2&2&0\\2&1&0&1&2\end{pmatrix}.$$

试把 M 表成(0—1)置换矩阵之和.

证 把S的所有线形r-排列分成组，使得同组的每个线形排列可以连接成同样的环形排列. 因为每组中恰含有r个线形排列，所以S的环形r-排列数$N=\frac{P(n,r)}{r}$. 当$r=n$时，S的环形排列数为$\frac{P(n,n)}{n}=(n-1)!$. ∎

【例 7.10】 (1) 10个男孩与5个女孩站成一排. 如果没有两个女孩相邻，问有多少种排法？

(2) 10个男孩和5个女孩站成一个圆圈. 如果没有两个女孩相邻，问有多少种排法？

解 把男孩子看成格子的分界，每两个男孩之间看成一个空格，把女孩看成不同的球，那么这个排列问题就对应于把不同的球放入空格，并且每个格只能放一个球的问题.

(1) 男孩组成格子的方法是$P(10,10)$种，对于任何一种组法，有11个位置放女孩，故女孩的排法数为$P(11,5)$. 根据乘法法则所求的排法数

$$N=P(10,10)\times P(11,5)=\frac{10!\times 11!}{6!}.$$

(2) 男孩组成格子的方法数是10个元素的环排列数，为$\frac{P(10,10)}{10}$. 而女孩放入10个格子的方法数为$P(10,5)$，由乘法法则总的排列数

$$N=\frac{P(10,10)}{10}\times P(10,5)=\frac{10!\times 9!}{5!}.$$

定义 7.3 从n元集S中无序选取的r个元素叫做S的一个r-组合，不同组合的总数记作$C(n,r)$.

定理 7.3 对一切正整数$n,r,n\geqslant r$，有

$$C(n,r)=\frac{P(n,r)}{r!}.$$

证 先从n元集中无序选择r个元素，选法数为$C(n,r)$，然后

方式，若其中任何两个事件产生的方式都不重叠，则事件“A_1 或 A_2 或 … 或 A_n”产生的方式是 $p_1 + p_2 + \cdots + p_n$ 种.

乘法法则 设事件 $A_1, A_2, \cdots, A_n$ 分别有 $p_1, p_2, \cdots, p_n$ 种产生的方式，若其中任何两个事件的产生都是相互独立的，则事件“A_1 与 A_2 与 … 与 A_n”的产生方式是 $p_1 \cdot p_2 \cdot \cdots \cdot p_n$ 种.

使用加法法则和乘法法则可以解决许多组合计数问题.

【例 7.5】 求 1400 的不同的正因子个数.

解 将 1400 做素因子分解得

$$1400 = 2^3 \times 5^2 \times 7.$$

1400 的任何正因子形式是 $2^i 5^j 7^k$，其中 $i, j, k \in N$，且 $i \leqslant 3, j \leqslant 2, k \leqslant 1$. 根据乘法法则，1400 的不同的正因子数

$$N = (3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 4 \times 3 \times 2 = 24.$$

【例 7.6】 已知从 1 到 n 的十进制正整数的总数字个数（不包括无效 0）是 1890，求 n.

解 易见 n 是一个三位数. 从 1 到 n，其中

一位数 9 个，数字总数为 9

二位数 90 个，数字总数为 2×90

三位数设为 x 个，数字总数为 $3x$

由加法法则得

$$3x + 2 \times 90 + 9 = 1890,$$

解得 $x = 567$. 因此 $n = 567 + 9 + 90 = 666$.

§7.2 排列和组合

先看下面的例子.

【例 7.7】 (1) 从 $\{1, 2, \cdots, 9\}$ 选取数字构成四位数，如果要求每位数字都不相同，问有多少种选法？

(2) 从 $\{1, 2, \cdots, 9\}$ 中选取数字构成四位数，问有多少种选法？

我们的做法是先选千位的数字，然后依次选择百位、十位、个位

取自同一组的选法数 $N_1 = 2C(n,2)$，

取自不同组的选法数 $N_2 = [C(n,1)]^2 = n^2$.

由加法法则，所求的选法数是 $2C(n,2) + n^2$. ∎

【例 7.13】 证明 k 个连续正整数的乘积可以被 $k!$ 整除.

证 设这 k 个连续正整数为 $n+1, n+2, \cdots, n+k$. 从 $n+k$ 个不同的球中选取 k 个球的方法数是 $C(n+k,k)$，即

$$N = \frac{(n+k)!}{n!k!} = \frac{(n+1)(n+2)\cdots(n+k)}{k!}.$$

显然 N 是正整数，所以 $k!$ 整除 $(n+1)(n+2)\cdots(n+k)$. ∎

定义 7.4 从多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$ 中有序选取的 r 个元素叫做 S 的一个 **r-排列**. 当 $r = n = n_1 + n_2 + \cdots + n_k$ 时也叫做 S 的一个**全排列**或简称为 S 的排列.

例如 $S = \{2 \cdot a, 1 \cdot b, 3 \cdot c\}$，则 $acab$, $abcc$ 是 S 的 4-排列，$abccca$ 是 S 的排列.

定理 7.4 设多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$，则 S 的 r-排列数是 k^r.

证 在构造 S 的一个 r-排列时，第一位有 k 种选法，第二位也有 k 种选法，…，第 r 位仍然有 k 种选法. 这是因为 S 中的每种元素都可以无限的重复，排列中每一位的选择都不依赖于以前各位的选择. 由乘法法则，不同的排列数是 k^r. ∎

由这个定理的证明立即可以得到下面的推论.

推论 设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$，且对一切 $i = 1, 2, \cdots, k$ 有 $n_i \geq r$，则 S 的 r-排列数为 k^r.

定理 7.5 设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$，且 $n = n_1 + n_2 + \cdots + n_k$，则 S 的排列数等于

$$\frac{n!}{n_1!n_2!\cdots n_k!},$$

我们把它简记为 $\binom{n}{n_1\ n_2\ \cdots\ n_k}$.

证 S 的一个排列就是它的 n 个元素的一个全排列. 因为 S 中有 n_1 个 a_1,在排列中要占据 n_1 个位置,这些位置的选法为$C(n,n_1)$种. 接下去,从剩下的 $n-n_1$ 个位置选择 n_2 个位置放 a_2,选法为 $C(n-n_1,n_2)$ 种.通过类似的分析可以得到放 a_3 的方法数为 $C(n-n_1-n_2,n_3)$,…,放 a_k 的方法数为 $C(n-n_1-n_2-\cdots-n_{k-1},n_k)$. 根据乘法法则,$S$ 的排列数为

$$
\begin{aligned}
N &= C(n,n_1)\cdot C(n-n_1,n_2)\cdot\cdots\cdot \\
&\quad C(n-n_1-n_2-\cdots-n_{k-1},n_k) \\
&= \frac{n!}{n_1!(n-n_1)!}\cdot\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdot\cdots\cdot \\
&\quad \frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!\quad 0!} \\
&= \frac{n!}{n_1!n_2!\cdots n_k!}.
\end{aligned}
$$

∎

【例 7.14】 求不多于 4 位的二进制数的个数.

解 这个问题相当于多重集$\{\infty\cdot 0,\infty\cdot 1\}$的 4- 排列问题. 由定理 7.4,所求的二进制数的个数是 $N=2^4=16$.

【例 7.15】 用两面红旗、三面黄旗一面接一面悬挂在一根旗杆上,问可以组成多少种不同的标志?

解 所求的标志数是多重集{2·红旗,3·黄旗}的排列数N. 由定理 7.5

$$N=\frac{5!}{2!\ 3!}=10.$$

关于多重集的排列数公式可以小结如下:

设 $S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$, $n=n_1+n_2+\cdots+n_k$,则 S 的 r- 排列数 N 满足:

(1) 若 $r>n$,则 $N=0$;

(2) 若 $r=n$,则 $N=\dfrac{n!}{n_1!\ n_2!\cdots n_k!}$;

(3) 若 $r < n$，且对一切 $i(i = 1,2,\cdots,k)$ 有 $n_i \geqslant r$，则 $N = k^r$；

(4) 若 $r < n$，且存在某个 $n_i < r$，则对 N 没有一般的求解公式，但 可以用其它的组合计数方法求解. 具体的求解方法将在后面几章讨论.

定义 7.5 设 S 是多重集，S 的含有 r 个元素的子多重集就叫做 S 的 **r-组合**.

例如 $S = \{2 \cdot a, 1 \cdot b, 3 \cdot c\}$，$S$ 的 2-组合有 5 个，它们是 $\{a,a\}$，$\{a,b\}$，$\{a,c\}$，$\{b,c\}$，$\{c,c\}$.

不难看出，如果多重集 S 有 n 个元素（包括重复的元素），则 S 的 n-组合只有一个，就是 S 本身. 如果 S 有 k 种不同的元素，则 S 的 1-组合恰有 k 个.

定理 7.6 设多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$，则 S 的 r-组合数是 $C(k + r - 1, r)$.

证 S 的任何一个 r-组合都具有下面的形式

$$\{x_1 \cdot a_1, x_2 \cdot a_2, \cdots, x_k \cdot a_k\},$$

其中 $x_1, x_2, \cdots, x_k$ 是非负整数，且满足

$$x_1 + x_2 + \cdots + x_k = r.$$

反之，对于每一组满足方程 $x_1 + x_2 + \cdots + x_k = r$ 的非负整数解 x_1，$x_2, \cdots, x_k$，$\{x_1 \cdot a_1, x_2 \cdot a_2, \cdots, x_k \cdot a_k\}$ 就是 S 的一个 r-组合. 所以多重集 S 的 r-组合数就等于方程 $x_1 + x_2 + \cdots + x_k = r$ 的非负整数解的个数. 下面我们将证明这种解的个数就等于多重集 $T = \{(k - 1) \cdot 0, r \cdot 1\}$ 的排列数.

给定 T 的一个排列，在这个排列中 $k - 1$ 个 0 把 r 个 1 分成 k 组. 从左边数起，我们把第一个 0 左边的 1 的个数记作 x_1，第一个 0 与第二个 0 之间的 1 的个数记作 x_2，…，最后一个 0 右边的 1 的个数记作 x_k. 则 $x_1, x_2, \cdots, x_k$ 都是非负整数，且它们的和是 r. 反之，给定方程 $x_1 + x_2 + \cdots + x_k = r$ 的一组非负整数解 $x_1, x_2, \cdots, x_k$，我们可以构造形如：

$$\underbrace{1\cdots1}_{x_1\text{个}1}\quad\underset{\text{第一个}0}{\overset{0}{\uparrow}}\quad\underbrace{1\cdots1}_{x_2\text{个}1}\quad\underset{\text{第二个}0}{\overset{0}{\uparrow}}\quad\cdots\quad\underset{\text{第}k-1\text{个}0}{\overset{0}{\uparrow}}\quad\underbrace{1\cdots1}_{x_k\text{个}1}$$

的排列。它就是多重集$\{(k-1)\cdot 0, r\cdot 1\}$的一个排列. 这就证明了多重集$T$的排列数等于方程$x_1+x_2+\cdots+x_k=r$的非负整数解的个数. 根据定理 7.5,$T$的排列数

$$N=\frac{(k-1+r)!}{(k-1)!\,r!}=C(k+r-1,r).$$ ▮

推论 1 设多重集$S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$,且对一切$i=1,2,\cdots,k$有$n_i\geqslant r$,则$S$的$r$-组合数为$C(k+r-1,r)$.

推论 2 设多重集$S=\{\infty\cdot a_1,\infty\cdot a_2,\cdots,\infty\cdot a_k\}$,$r\geqslant k$,则$S$中每个元素至少取一个的$r$-组合数为$C(r-1,k-1)$.

证 任取一个所求的r-组合,从中拿走元素$a_1,a_2,\cdots,a_k$,就得到一个S的$(r-k)$-组合;反之,对于S的一个$(r-k)$-组合,加入元素$a_1,a_2,\cdots,a_k$,就得到所求的组合. 所以S中每个元素至少取一个的r-组合数就是S的$(r-k)$-组合数,由定理 7.6 所求的r-组合数是

$$\begin{aligned}N&=C(k+(r-k)-1,r-k)=C(r-1,r-k)\\&=C(r-1,k-1).\end{aligned}$$ ▮

【例 7.16】 试确定多重集$S=\{1\cdot a_1,\infty\cdot a_2,\cdots,\infty\cdot a_k\}$的$r$-组合数.

解 把S的r-组合分成两类.

包含a_1的r-组合:这种组合数等于多重集$S=\{\infty\cdot a_2,\infty\cdot a_3,\cdots,\infty\cdot a_k\}$的$(r-1)$-组合数,即

$$\begin{aligned}N_1&=C((k-1)+(r-1)-1,r-1)\\&=C(k+r-3,r-1).\end{aligned}$$

不包含a_1的r-组合:这种组合数等于多重集$\{\infty\cdot a_2,\infty\cdot a_3,\cdots,\infty\cdot a_k\}$的$r$-组合数,即

$$N_2=C((k-1)+r-1,r)=C(k+r-2,r).$$

由加法法则，所求的 r- 组合数

$$N = N_1 + N_2 = C(k+r-3, r-1) + C(k+r-2, r).$$

关于多重集的组合数公式可以小结如下.

设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$，$n = n_1 + n_2 + \cdots + n_k$，则 S 的 r- 组合数 N 满足：

(1) 若 $r > n$，则 $N = 0$；

(2) 若 $r = n$，则 $N = 1$；

(3) 若 $r < n$，且对一切 $i(i = 1, 2, \cdots, k)$ 有 $n_i \geqslant r$，则

$$N = C(k+r-1, r);$$

(4) 若 $r < n$，且存在某个 $n_i < r$，则对 N 没有一般的求解公式，但可以用其它的组合计数方法求解，具体的求解方法将在后面几章讨论.

§7.3 二项式定理与组合恒等式

组合数 $C(n,k)$，也记作 $\binom{n}{k}$，叫做**二项式系数**. 关于 $\binom{n}{k}$，已经证明了下面的结果：

对任意的 $n, k \in N$ 有

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!}, & k \leqslant n, \\ 0, & k > n, \end{cases}$$

$$\binom{n}{k} = \binom{n}{n-k}, \qquad n \geqslant k. \tag{7.1}$$

利用这些结果不难得到下面的等式：

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}, \qquad n, k \in Z^+. \tag{7.2}$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \qquad n, k \in Z^+. \tag{7.3}$$

等式 7.3 叫做 Pascal 公式，也叫杨辉三角形公式，利用它可以证明二项式定理.

定理 7.7 (二项式定理) 设 n 是正整数，对一切 x 和 y 有

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}.$$

证 用数学归纳法.

当 $n=1$ 时

左边 $=(x+y)^1=x+y$,

右边 $=\sum_{k=0}^{1}\binom{1}{k}x^k y^{1-k}=\binom{1}{0}x^0y^1+\binom{1}{1}x^1y^0=y+x.$

命题为真. 假设等式对任意的正整数 n 都成立，则

$$\begin{aligned}
&(x+y)^{n+1}=(x+y)(x+y)^n\\
&=y\left[\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right]+x\left[\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right]\\
&=\binom{n}{0}y^{n+1}+\sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1}+\sum_{k=0}^{n-1}\binom{n}{k}x^{k+1}y^{n-k}+\binom{n}{n}x^{n+1}\\
&=\binom{n}{0}y^{n+1}+\sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1}+\sum_{k=1}^{n}\binom{n}{k-1}x^k y^{n-k+1}\\
&\quad+\binom{n+1}{n+1}x^{n+1}\\
&=\binom{n+1}{0}y^{n+1}+\sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]x^k y^{n-k+1}+\binom{n+1}{n+1}x^{n+1}\\
&=\binom{n+1}{0}y^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}x^k y^{n+1-k}+\binom{n+1}{n+1}x^{n+1}\\
&=\sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}.
\end{aligned}$$

由归纳法可知定理对一切正整数 n 都成立. ∎

推论 1 设 n 是正整数，对一切 x 有

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

证 在二项式定理中令 $y=1$ 即可. ▮

推论 2 对任何正整数 n 有

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}=2^n. \tag{7.4}$$

证 在二项式定理中令 $x=y=1$ 即可. ▮

推论 3 对任何正整数 n 有

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\cdots+(-1)^n\binom{n}{n}=0. \tag{7.5}$$

证 在二项式定理中令 $x=-1, y=1$ 即可. ▮

在二项式定理的展开式中每一项的系数都是组合数. 推论 2 和推论 3 是关于二项式系数的等式,实际上也是关于组合数的等式. 可以从组合分析的角度来解释和证明这两个推论.

对任何正整数 n 和自然数 k, $\binom{n}{k}$ 表示 n 元集的 k 子集个数. 7.4 式左边计数了 n 元集的所有子集数. 从另一方面考虑这个计数问题. 在构成 n 元集的子集时, n 元集的每个元素都可以有两种选择,属于这个子集或不属于这个子集. 根据乘法法则不同的子集有 2^n 个.

将等式 7.5 中带负号的项移到右边就得到

$$\binom{n}{0}+\binom{n}{2}+\cdots=\binom{n}{1}+\binom{n}{3}+\cdots. \tag{7.5$'$}$$

这说明 n 元集($n \in Z^+$)的偶子集个数与奇子集个数相等. 任取 n 元集 S 中的一个元素 x,对于 S 的任何偶子集 $A \subseteq S$,若 $x \in A$,则令 $B = A - \{x\}$;若 $x \notin A$,则令 $B = A \cup \{x\}$. B 显然是 S 的奇子集,不难证明这是所有的偶子集与所有的奇子集之间的一一对应. 所以 S 的偶子集数与奇子集数相等.

等式 7.1 到 7.5 都叫做组合恒等式. 下面再给出一些常见的组

合恒等式.

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}, \qquad n \in Z^+. \tag{7.6}$$

$$\sum_{k=1}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2}, \qquad n \in Z^+. \tag{7.7}$$

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k},$$

$$n,r,k \in Z^+,\ r \geqslant k. \tag{7.8}$$

$$\sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r},$$

$$m,n,r \in N,\ r \leqslant \min\{m,n\}. \tag{7.9}$$

$$\sum_{k=0}^{m}\binom{m}{k}\binom{n}{k} = \binom{m+n}{m}, \qquad m,n \in N. \tag{7.10}$$

$$\sum_{l=0}^{n}\binom{l}{k} = \binom{n+1}{k+1}, \qquad n,k \in N. \tag{7.11}$$

$$\sum_{l=0}^{k}\binom{n+l}{l} = \binom{n+k+1}{k}, \qquad n,k \in N. \tag{7.12}$$

我们选证其中的一部分.

证等式 7.6.

对 $k = 1,2,\cdots,n$,有

$$k\binom{n}{k} = k\,\frac{n}{k}\binom{n-1}{k-1} = n\binom{n-1}{k-1},$$

然后代入等式 7.6 的左边得

$$\sum_{k=1}^{n} k\binom{n}{k} = \sum_{k=1}^{n} n\binom{n-1}{k-1} = n\sum_{k=1}^{n}\binom{n-1}{k-1} = n\sum_{k=0}^{n-1}\binom{n-1}{k} = n2^{n-1}.$$

证等式 7.7.

由二项式定理有

$$(1+x)^n = 1 + \sum_{k=1}^{n} \binom{n}{k} x^k.$$

对上式两边微商得

$$n(1+x)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k x^{k-1}.$$

两边同乘 x 得

$$nx(1+x)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k x^k.$$

然后两边再次微商得

$$n(1+x)^{n-1} + nx(n-1)(1+x)^{n-2} = \sum_{k=1}^{n} \binom{n}{k} k^2 x^{k-1}.$$

在上式中令 $x=1$,然后化简得

$$n(n+1)2^{n-2} = \sum_{k=1}^{n} \binom{n}{k} k^2.$$

证等式 7.9.

由二项式定理得

$$(1+x)^m = \sum_{k=0}^{m} \binom{m}{k} x^k, \quad (1+x)^n = \sum_{l=0}^{n} \binom{n}{l} x^l,$$

因此有

$$(1+x)^{m+n} = \left[\sum_{k=0}^{m} \binom{m}{k} x^k\right] \left[\sum_{l=0}^{n} \binom{n}{l} x^l\right].$$

比较两边 x^r 的系数,左边是$\binom{m+n}{r}$,右边是$\sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k}$.

证等式 7.11.

使用组合分析的方法. 令 $S = \{a_1, a_2, \cdots, a_{n+1}\}$, 要从 S 中选取 $k+1$ 元子集,我们把这些子集分类:

含 a_1 的子集是$\binom{n}{k}$个;

不含 a_1 而含 a_2 的子集是 $\binom{n-1}{k}$ 个；

不含 a_1 和 a_2 但含 a_3 的子集是 $\binom{n-2}{k}$ 个；

……

不含 $a_1,\cdots,a_n$ 而含 a_{n+1} 的子集是 $\binom{0}{k}$ 个.

由加法法则，等式 7.11 成立.

以上证明组合恒等式的主要方法可以归纳如下：

代数方法. 通过代入组合数的值或已知的组合恒等式后进行计算或化简，使得等式两边相等.

使用二项式定理比较展开式中 x^r 的系数，或令 x 和 y 为某个特定的值.

利用幂级数的微商或积分等.

数学归纳法.

使用组合分析方法，说明等式两边都是对同一组合问题的计数.

下边考虑一个和组合恒等式密切相关的组合计数问题 —— 非降路径问题.



图 7.1

如图 7.1，从 $(0,0)$ 点开始，水平向右走一步为 x，垂直向上走一步为 y，则走到 (m,n) 点水平向右要走 m 步，垂直向上要走 n 步. 每一条从 $(0,0)$ 点到 (m,n) 的非降路径就是 m 个 x 和 n 个 y 的一个排列. 反之，给了 m 个 x 和 n 个 y 的一个排列就唯一地确定了一条从 $(0,0)$ 点到 (m,n) 点的非降路径. 于是从 $(0,0)$ 点到 (m,n) 点的非降路径数等于 m 个 x，n 个 y 的排列数，即 $\binom{m+n}{m}$.

一般地，由(a,b)点到(m,n)点的非降路径数等于从$(0,0)$点到$(m-a,n-b)$点的非降路径数，即$\binom{m+n-(a+b)}{m-a}$. 而从(a,b)点经过(c,d)点而到达(m,n)点的非降路径数根据乘法法则应该等于从(a,b)点到(c,d)点的非降路径数乘以从(c,d)点到(m,n)点的非降路径数，即$\binom{c+d-(a+b)}{c-a}\binom{m+n-(c+d)}{m-c}$.

如果对非降路径附加其它的限制条件，可以采用反射的原则来处理. 例如，求从$(0,0)$点到(n,n)点的除端点外不接触直线$y=x$的非降路径数. 先考虑直线$y=x$下面的路径，这种路径都是从$(0,0)$点出发，经$(1,0)$点及$(n,n-1)$点而到达(n,n)点的. 可以把它们看作是从$(1,0)$点出发到达$(n,n-1)$点不接触$y=x$直线的路径.

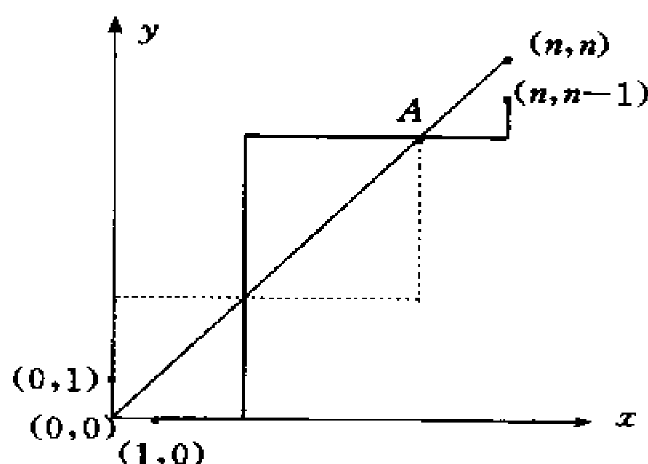


图 7.2

从$(1,0)$点到$(n,n-1)$点的所有非降路径数是$\binom{2n-2}{n-1}$. 对其中任意一条接触直线$y=x$的路径，可以把它从最后离开这条直线的点（图 7.2 中的A点）到$(1,0)$点之间的部分关于$y=x$直线作一个反射（图 7.2 中的虚线部分），就得到一条从$(0,1)$点出发经过A点到达$(n,n-1)$点的非降路径. 反之，任何一条从$(0,1)$出发，穿过对角线$y=x$而到达$(n,n-1)$点的非降路径，也可以通过这样的反射对应到一条从$(1,0)$点出发接触到对角线$y=x$而到达$(n,n-1)$点的非降路径. 从$(0,1)$点到达$(n,n-1)$点的非降路径数是$\binom{2n-2}{n}$，从而在直线$y=x$下方的非降路径数是$\binom{2n-2}{n-1}-\binom{2n-2}{n}$. 由对称性可知，

所求的非降路径数是

$$2\left[\binom{2n-2}{n-1}-\binom{2n-2}{n}\right]=\frac{2}{n}\binom{2n-2}{n-1}=\frac{1}{2n-1}\binom{2n}{n}.$$

利用非降路径的计数可以证明组合恒等式.

【例 7.17】 用非降路径的计数证明公式 7.4.

证 如图 7.3，$\binom{n}{k}$ 计数了从 $(0,0)$ 点到 $(k,n-k)$ 点的非降路径，其中 $k=0,1,\cdots,n$，所以公式左边是从 $(0,0)$ 出发到达直线 $y=-x+n$ 的所有非降路径数. 另一方面，从 $(0,0)$ 到直线 $y=-x+n$ 的非降路径都是 n 步长，每一步或是 x 或是 y，有两种选择. 由乘法法则，n 步长的不同选择方法的总数为 2^n，这也是从 $(0,0)$ 到直线 $y=-x+n$ 的非降路径的总数.

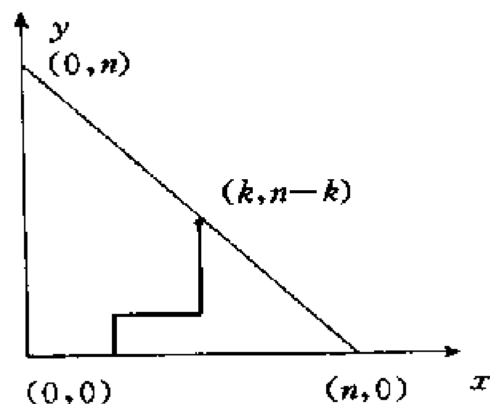


图 7.3

【例 7.18】 求集合 $\{1,2,\cdots,n\}$ 上的单调递增函数的个数.

解 任给集合 $\{1,2,\cdots,n\}$ 上的一个单调递增函数，我们可以作一条对应的折线(参看图 7.4). 以横坐标代表 x，纵坐标代表 $f(x)$，在图中可以得到 n 个点：$(1,f(1))$，$(2,f(2))$，…，$(n,f(n))$. 从 $(1,1)$ 点出发，向上做连线到 $(1,f(1))$ 点. 如果 $f(2)=f(1)$，则继续向右连线到 $(2,f(2))$ 点；如果 $f(2)>f(1)$，则由 $(1,f(1))$ 点再向右经过 $(2,f(1))$ 点，再向上连线到 $(2,f(2))$ 点. 按

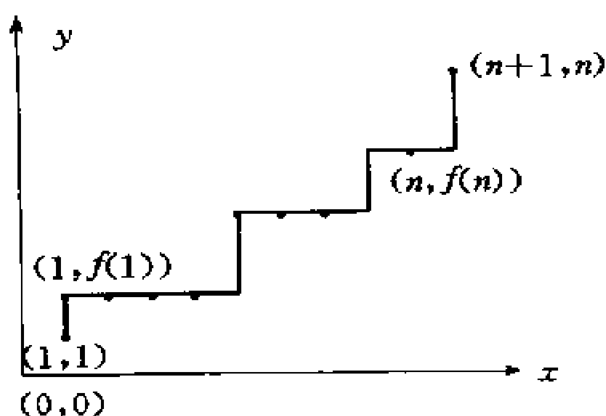


图 7.4

照这种方法一直将折线连到$(n,f(n))$点. 若$f(n)=n$,就将折线向右连到$(n+1,n)$点;若$f(n)<n$,则向右经$(n+1,f(n))$点再向上连线到$(n+1,n)$点. 这样就得到一条从$(1,1)$点到$(n+1,n)$点的非降路径. 不难看出,所求的单调递增函数与这种非降路径之间存在着一一对应,因此集合$\{1,2,\cdots,n\}$上的单调函数有$\binom{2n-1}{n}$个.

§7.4 多项式定理

多项式定理是二项式定理的推广.

定理 7.8 (多项式定理)

设n是正整数,则对一切实数$x_1,x_2,\cdots,x_t$有

$$(x_1+x_2+\cdots+x_t)^n=\sum\binom{n}{n_1\ n_2\ \cdots\ n_t}x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t},$$

其中求和是对满足方程$n_1+n_2+\cdots+n_t=n$的一切非负整数负n_1,$n_2,\cdots,n_t$来求.

证 $(x_1+\cdots+x_t)^n$是n个因式$(x_1+\cdots+x_t)$相乘. 每个因式相乘时可以分别贡献x_1或$x_2,\cdots$,或x_t,有t种选择. 所以乘积展开式中共有t^n个项(包括同类项),且每一项都是$x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}$的形式,其中$n_1,n_2,\cdots,n_t$为非负整数并且满足$\sum\limits_{i=1}^{t}n_i=n$. 我们在$n$个因式$(x_1+\cdots+x_t)$中选取$n_1$个贡献$x_1$,在剩下的$n-n_1$个因式$(x_1+\cdots+x_t)$中选取$n_2$个贡献$x_2,\cdots$,在$(n-n_1-\cdots-n_{t-1})$个因式$(x_1+\cdots+x_t)$中选取$n_t$个贡献$x_t$. 于是项$x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}$出现的次数为

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_{t-1}}{n_t}$$

$$=\frac{n!}{n_1!(n-n_1)!}\cdot\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdot\cdots\cdot\frac{(n-n_1-\cdots-n_{t-1})!}{n_t!(n-n_1-\cdots-n_t)!}$$

$$=\frac{n!}{n_1!n_2!\cdots n_t!}=\binom{n}{n_1\ n_2\ \cdots\ n_t}.$$ ∎

推论 1 $(x_1+\cdots+x_t)^n$ 的展开式在合并同类项以后不同的项数是$\binom{n+t-1}{n}$.

证 $(x_1+\cdots+x_t)^n$ 的展开式中任何一项都是 $x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}$ 的形式,其中 $n_1+n_2+\cdots+n_t=n$. 每一项对应于方程 $n_1+n_2+\cdots+n_t=n$ 的一组非负整数解,所以合并同类项后不同的项数等于这个方程的非负整数解的个数$\binom{n+t-1}{n}$. ∎

推论 2 $\sum\binom{n}{n_1\ n_2\ \cdots\ n_t}=t^n$,其中求和是对方程 $n_1+n_2+\cdots+n_t=n$ 的一切非负整数解来求和.

证 在多项式定理中令 $x_1=x_2=\cdots=x_t=1$ 即可. ∎

多项式定理是二项式定理的推广,在多项式定理中令 $t=2$ 就得到了二项式定理. 多项式定理中的系数$\binom{n}{n_1\ n_2\ \cdots\ n_t}$叫做**多项式系数**. 下面我们进一步分析它的组合意义.

$\binom{n}{n_1\ n_2\ \cdots\ n_t}$是:

多重集 $S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_t\cdot a_t\}$ 的全排列数(定理 7.5).

把 n 个有区别的球放到 t 个有区别的盒子里,并且要求第一个盒子含有 n_1 个球,第二个盒子含有 n_2 个球,…,第 t 个盒子含有 n_t 个球的放球方案数.

把 n 元集划分成 t 个有序子集(允许空子集)并且要求第一个子集含 n_1 个元素,第二个子集含 n_2 个元素,…,第 t 个子集含 n_t 个元素的划分方案数.

关于放球问题及有序子集划分问题的证明留给读者.

【例 7.19】 求$(2x_1-3x_2+5x_3)^6$中$x_1^3x_2x_3^2$项的系数.

解 $\binom{6}{3\ 1\ 2}2^3\cdot(-3)\cdot 5^2=\frac{6!}{3!1!2!}8\cdot(-3)\cdot 25=-36000.$

【例 7.20】 证明

$$\binom{n}{n_1\ n_2\ \cdots\ n_t}=\binom{n-1}{n_1-1\quad n_2\cdots n_t}+\binom{n-1}{n_1\quad n_2-1\cdots n_t}+\cdots$$
$$+\binom{n-1}{n_1\ n_2\cdots n_t-1}.$$

证 等式左边计数了n个不同的球放到t个不同的盒子里并且要求第一个盒子里含有n_1个球,第二个盒子里含有n_2个球,…,第t个盒子里含有n_t个球的方案数.将所有的放球方案作下面的分类:

任取一个球,比如说a_1.

a_1放到第一个盒子里方案数为$\binom{n-1}{n_1-1\quad n_2\cdots n_t}$;

a_1放到第二个盒子里方案数为$\binom{n-1}{n_1\quad n_2-1\cdots n_t}$;

……

a_1放到第t个盒子里方案数为$\binom{n-1}{n_1\ n_2\cdots n_t-1}$.

由加法法则总方案数为

$$\binom{n-1}{n_1-1\quad n_2\cdots n_t}+\binom{n-1}{n_1\quad n_2-1\cdots n_t}+\cdots+\binom{n-1}{n_1\ n_2\cdots n_t-1}.$$

【例 7.21】 设k为正整数,证明$\frac{(k!)!}{[(k-1)!]!^k}$是整数.

证 令$n_1=n_2=\cdots=n_k=(k-1)!$,则$\sum_{i=1}^{k}n_i=k(k-1)!=k!$.考虑多项式系数

$$\binom{\sum_{i=1}^{k} n_i}{n_1\ n_2\ \cdots\ n_k} = \binom{k!}{(k-1)!\ (k-1)!\ \cdots\ (k-1)!}$$

$$= \frac{(k!)!}{[(k-1)!]!^{k}}.$$

由于多项式系数是组合计数问题的计数结果，必为整数.

习　题　七

1. 某产品的加工需要 5 道工序，问

(1) 加工工序共有多少种排法?

(2) 其中某工序必须先加工，有多少种排法?

(3) 其中某工序不能放在最后加工，又有多少种排法?

2. 现有 100 件产品，从其中任意抽出 3 件，

(1) 共有多少种不同的抽法?

(2) 如果 100 件产品中有 2 件次品，抽出的产品中恰好有 1 件次品的抽法有多少种?

(3) 如果 100 件产品中有 2 件次品，抽出的产品中至少有 1 件次品的抽法有多少种?

3. 有纪念章 4 枚，纪念册 6 本，赠给 10 位同学，每人得一件，共有多少种不同的送法?

(1) 如果纪念章是彼此不同的，纪念册也是彼此不同的；

(2) 如果纪念章是相同的，纪念册也是相同的.

4. (1) 从整数 1,2,…,100 中选出两个数，使得它们的差正好是 7，有多少种不同的选法?

(2) 如果选出的两个数之差小于等于 7，又有多少种不同的选法?

5. 从一个 8 × 8 的棋盘中选出两个相邻的方格，问有多少种选法?在这里规定两个方格在同一行或同一列上相邻才是相邻的方格.

6. (1) 把字母 a,b,c,d,e,f 进行排列，使得字母 b 总是紧跟在字母 e 的左边，问有多少种排法?

(2) 若在排列中使得字母 b 总在字母 e 的左边，又有多少种排法？

7. 一个教室有两排座位，每排8个．有14个学生，其中的5个人总坐在前一排，另外有4个人总坐在后一排，问有多少种排法？

8. 书架上有9本不同的书，其中4本是红皮的，5本是黑皮的．

(1) 9本书的排列有多少种？

(2) 若黑皮的书都排在一起，这样的排列有多少种？

(3) 若黑皮的书排在一起，红皮的书也排在一起，这样的排列有多少种？

(4) 若黑皮的书与红皮的书必须相间，这样的排列又有多少种？

9. 书架上有24卷百科全书，从其中选5卷使得任何2卷都不相继，这样的选法有多少种？

10. 证明从 $\{1,2,\cdots,n\}$ 中任选 m 个数排成一个圆圈的方法数是 $\frac{n!}{m(n-m)!}$.

11. 考虑集合 $\{1,2,\cdots,n+1\}$ 的非空子集.

(1) 证明最大元素恰好是 j 的子集数是 2^{j-1}；

(2) 利用(1)的结论证明

$$1+2+2^2+\cdots+2^m=2^{m+1}-1.$$

11. (1) 从200辆汽车中选取30辆作安全试验，同时选取30辆作防污染的试验，问有多少种选法？

(2) 有多少种选法使得正好5辆汽车同时经受两种试验？

12. (1) 15名篮球运动员被分配到 A,B,C 三个组，使得每组有5名运动员，那么有多少种分法？

(2) 15名篮球运动员被分成三个组使得每组有5名运动员，那么有多少种分法？

13. 在三年级和四年级各有50名学生，其中有25名男生和25名女生，要选出8名代表使得其中有4名女生和3名低年级学生，这样的选法有多少种？

14. 从整数1,2,…,1000中选取三个数使得它们的和正好被4整除，问有多少种选法？

15. 从去掉大小王的52张扑克牌中选5张牌，求

(1) 使得没有 A 但有2张 K 的方法数；

(2) 使得其中有红桃 A，其它4张牌是顺子的方法数.

16. 设$S=\{1,2,\cdots,n+1\}$，从S中选择3个数构成有序三元组$\langle x,y,z\rangle$使得$z>x$且$z>y$.

(1) 证明：若$z=k+1$，则这样的有序三元组恰为k^2个；

(2) 将所有有序三元组按$x=y$，$x<y$，$x>y$分成A,B,C三组.证明

$$|A|=\binom{n+1}{2},\ |B|=|C|=\binom{n+1}{3};$$

(3) 由(1)和(2)证明恒等式

$$1^2+2^2+3^2+\cdots+n^2=\binom{n+1}{2}+2\binom{n+1}{3}.$$

17. $S=\{\infty\cdot a_1,\infty\cdot a_2,\cdots,\infty\cdot a_k\}$，求$S$的各种大小的子集总数.

18. $S=\{1\cdot a_1,1\cdot a_2,\cdots,1\cdot a_t,\infty\cdot a_{t+1},\infty\cdot a_{t+2},\cdots,\infty\cdot a_k\}$，求$S$的$r$-组合数.

19. 有红球4个，黄球3个，白球3个，把它们排成一条直线，问有多少种排法？

20. 从$\{\infty\cdot 0,\infty\cdot 1,\infty\cdot 2\}$中取$n$个数作排列，若不允许相邻位置的数相同，问有多少种排法？

21. 小于10^n且各位数字从左到右具有非降顺序的正整数有多少个？

22. 把22本不同的书分给5个学生使得其中的2名学生各得5本，而另外的3名学生各得4本，这样的分法有多少种？

23. (1) 把r只相同的球放到n个不同的盒子里($n\leqslant r$)，没有空盒，证明放球的方法数是$C(r-1,n-1)$.

(2) 把r只相同的球放到n个不同的盒子里，每个盒子至少包含q个球，问有多少种方法？

24. 给出多重集$\{2\cdot a,\ 1\cdot b,\ 3\cdot c\}$所有的3-排列和3-组合.

25. 证明由数字1,1,2,3,3,4所组成的4位数的个数是102.

26. 用二项式定理展开$(2x-y)^7$.

27. $(3x-2y)^{18}$的展开式中x^5y^{13}的系数是什么？x^8y^9的系数是什么？

28. 证明 $\sum_{k=0}^{n}\binom{n}{k}2^k=3^n$.

29. 证明 $\sum_{k=0}^{n}(-1)^k\binom{n}{k}3^{n-k}=2^n$.

30. 证明以下组合恒等式：

(1) $\sum_{k=1}^{n+1} \frac{1}{k}\binom{n}{k-1} = \frac{2^{n+1}-1}{n+1}$；

(2) $\sum_{k=0}^{n}(k+1)\binom{n}{k} = 2^{n-1}(n+2)$；

(3) $\sum_{k=0}^{n} \frac{2^{k+1}}{k+1}\binom{n}{k} = \frac{3^{n+1}-1}{n+1}$；

(4) $\sum_{k=1}^{n}(-1)^{k-1}\frac{1}{k}\binom{n}{k} = 1+\frac{1}{2}+\cdots+\frac{1}{n}$.

31. 求和：

(1) $\sum_{k=0}^{n}\binom{n}{k}r^k$，$r$ 为实数，n 为正整数；

(2) $\sum_{k=0}^{n}(-1)^k\frac{1}{k+1}\binom{n}{k}$；

(3) $\sum_{k=0}^{n}\binom{2n-k}{n-k}$.

32. 证明 $\sum_{k=0}^{n}\frac{(-1)^k}{m+k+1}\binom{n}{k} = \frac{n!m!}{(n+m+1)!}$.

33. 证明 $\sum_{k=0}^{n-1}\binom{n}{k}\binom{n}{k+1} = \frac{(2n)!}{(n-1)!(n+1)!}$.

34. 证明 $\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k+1}\binom{n}{k} = \frac{n}{n+1}$.

35. 证明 $\sum_{k=2}^{n-1}(n-k)^2\binom{n-1}{n-k} = n(n-1)2^{n-3}-(n-1)^2$.

36. 求和：

(1) $\sum_{k=0}^{m}\binom{n-k}{m-k}$；

(2) $\sum_{k=0}^{m}\binom{u}{k}\binom{v}{m-k}$.

37. 用多项式定理展开 $(x_1+x_2+x_3)^4$.

38. 确定在$(x_1-x_2+2x_3-2x_4)^8$ 的展开式中 $x_1^2x_2^3x_3x_4^2$ 项的系数.

39. (1) 给定正整数 n，证明

$$\sum (-1)^{a+b}\binom{n}{a\ b\ c\ d}=0,$$

其中求和是对方程 $a+b+c+d=n$ 的一切非负整数解来求和；

(2) 如何将以上命题一般化？

40. 设 p 是一个素数，$p\neq 2$，则当 $\binom{2p}{p}$ 被 p 整除时余数是 2.

41. 证明把 n 个有区别的球放到 t 个有区别的盒子里，并且要求第一个盒子里含 n_1 个球，第二个盒子里含 n_2 个球，…，第 t 个盒子里含 n_t 个球的放球方法数是 $\binom{n}{n_1\ n_2\ \cdots\ n_t}$.

42. 证明把 n 元集划分成 t 个有序子集（允许空子集）并且要求第一个子集含 n_1 个元素，第二个子集含 n_2 个元素，…，第 t 个子集含 n_t 个元素的划分方案数是 $\binom{n}{n_1\ n_2\ \cdots\ n_t}$.

43. (1) 设 p 是素数，且 $\binom{p}{n_1\ n_2\ \cdots\ n_t}\neq 1$，则 p 整除 $\binom{p}{n_1\ n_2\ \cdots\ n_t}$；

(2) (Fermat 小定理) 通过把 n^p 写成 $(1+1+\cdots+1)^p$ 的形式，证明 p 整除 n^p-n.

44. 用非降路径的方法证明组合恒等式 7.9，7.11 和 7.12.

45. 用非降路径的方法证明

$$\sum_{k=0}^{m}\binom{n-k}{m-k}\binom{r+k}{k}=\binom{n+r+1}{m}.$$

46. 计数从 $(0,0)$ 点到 (n,n) 点的不穿过直线 $y=x$ 的非降路径数.

第八章　组合计数方法

本章主要讨论递推方程和生成函数在组合计数中的应用.

§8.1　递推方程的公式解法

定义 8.1　给定一个数的序列 $H(0), H(1), \cdots, H(n), \cdots$，用等号把 $H(n)$ 和某些个 $H(i), 0 \leqslant i < n$，联系起来的等式叫做**递推方程**.

利用递推方程和初值在某些情况下可以求出序列的通项表达式 $H(n)$. 通常 $H(n)$ 总是代表了某个组合计数问题的解，从而可以利用递推方程来解决组合计数问题.

最简单的一类递推方程是常系数线性齐次递推方程.

定义 8.2　下面的等式

$$H(n) - a_1 H(n-1) - a_2 H(n-2) - \cdots - a_k H(n-k) = 0,$$
$$n \geqslant k,\ a_1, a_2, \cdots, a_k \text{ 是常数}, a_k \neq 0 \qquad (8.1)$$

称作 k **阶常系数线性齐次递推方程**.

定义 8.3　方程

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k = 0 \qquad (8.2)$$

称为递推方程 8.1 的**特征方程**. 它的 k 个根 $q_1, q_2, \cdots, q_k$ 称为递推方程的**特征根**，其中 $q_i (i = 1, 2, \cdots, k)$ 是复数.

不难看出，因为 $a_k \neq 0$，所以 0 不是递推方程 8.1 的特征根.

定理 8.1　设 q 是一个非零复数，则 $H(n) = q^n$ 是递推方程 8.1 的一个解当且仅当 q 是它的一个特征根.

证　$H(n) = q^n$ 是递推方程程 8.1 的解

$$\Leftrightarrow q^n - a_1 q^{n-1} - a_2 q^{n-2} - \cdots - a_k q^{n-k} = 0$$

$$\Leftrightarrow q^{n-k}(q^k - a_1 q^{k-1} - a_2 q^{k-2} - \cdots - a_k) = 0$$

$$\Leftrightarrow q^k - a_1 q^{k-1} - a_2 q^{k-2} - \cdots - a_k) = 0 \quad (q \neq 0)$$

$\Leftrightarrow q$ 是递推方程 8.1 的特征根. ∎

定理 8.2　设 $h_1(n)$ 和 $h_2(n)$ 是递推方程 8.1 的两个解，c_1 和 c_2 是任意常数，则 $c_1h_1(n)+c_2h_2(n)$ 也是递推方程 8.1 的解.

证　把 $c_1h_1(n)+c_2h_2(n)$ 代入 8.1 式的左边得

$$
\begin{aligned}
& [c_1h_1(n)+c_2h_2(n)]-a_1[c_1h_1(n-1)+c_2h_2(n-1)] \\
& -\cdots-a_k[c_1h_1(n-k)+c_2h_2(n-k)] \\
= & [c_1h_1(n)-a_1c_1h_1(n-1)-\cdots-a_kc_1h_1(n-k)] \\
& +[c_2h_2(n)-a_1c_2h_2(n-1)-\cdots-a_kc_2h_2(n-k)] \\
= & c_1[h_1(n)-a_1h_1(n-1)-\cdots-a_kh_1(n-k)] \\
& +c_2[h_2(n)-a_1h_2(n-1)-\cdots-a_kh_2(n-k)] \\
= & 0,
\end{aligned}
$$

所以 $c_1h_1(n)+c_2h_2(n)$ 是递推方程 8.1 的解. ∎

由定理 8.1 和 8.2 可以知道，如果 $q_1,q_2,\cdots,q_k$ 是递推方程 8.1 的特征根，且 $c_1,c_2,\cdots,c_k$ 是任意常数，那么

$$H(n)=c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$$

是递推方程 8.1 的解.

定义 8.4　如果对于递推方程 8.1 的每个解 $h(n)$ 都可以选择一组常数 $c'_1,c'_2,\cdots,c'_k$ 使得

$$h(n)=c'_1q_1^n+c'_2q_2^n+\cdots+c'_kq_k^n$$

成立，则称 $c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$ 是递推方程 8.1 的通解，其中 c_1，$c_2,\cdots,c_k$ 是任意常数.

定理 8.3　设 $q_1,q_2,\cdots,q_k$ 是递推方程 8.1 的不相等的特征根，则

$$H(n)=c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$$

是递推方程 8.1 的通解.

证　由前边的分析可知 $H(n)$ 是递推方程 8.1 的解. 设 $h(n)$ 是该递推方程的任意一个解，则 $h(n)$ 由 k 个初值 $h(0)=b_0,h(1)=b_1$，

$\cdots, h(k-1)=b_{k-1}$ 唯一地确定，考虑下面的方程组

$$\begin{cases} c_1+c_2+\cdots+c_k=b_0, \\ c_1q_1+c_2q_2+\cdots+c_kq_k=b_1, \\ \cdots \\ c_1q_1^{k-1}+c_2q_2^{k-1}+\cdots+c_kq_k^{k-1}=b_{k-1}. \end{cases} \tag{8.3}$$

如果方程组 8.3 有唯一解 $c'_1, c'_2, \cdots, c'_k$，这说明可以找到 k 个常数 c'_1, $c'_2, \cdots, c'_k$ 使得

$$h(n)=c'_1q_1^n+c'_2q_2^n+\cdots+c'_kq_k^n$$

成立，从而证明了 $c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$ 是该递推方程的通解.

考察方程组 8.3，它的系数行列式是

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ q_1 & q_2 & \cdots & q_k \\ q_1^2 & q_2^2 & \cdots & q_k^2 \\ \cdots & & & \\ q_1^{k-1} & q_2^{k-1} & \cdots & q_k^{k-1} \end{vmatrix},$$

这是著名的 Vandermonde 行列式，其值为

$$\prod_{1\leqslant i<j\leqslant k}(q_j-q_i).$$

因为当 $i\neq j$ 时 $q_i\neq q_j$，所以行列式的值不等于 0，这也就是说方程组 8.3 有唯一解. ∎

【例 8.1】 关于 Fibonacci 数列的问题是一个古老的问题，是在 1202 年提出来的. 这个问题是：把一对兔子（雌、雄各一只）在某年的开始放到围栏中，每个月这对兔子都生出一对新兔，其中雌、雄各一只. 由第二个月开始，每对新兔每个月也生出一对新兔，也是雌、雄各一只，问一年后围栏中有多少对兔子？

解 对于 $n=1,2,\cdots$，令 $f(n)$ 表示第 n 个月开始时围栏中的兔子对数. 显然有 $f(1)=1$，$f(2)=2$. 在第 n 个月的开始，那些第 $n-1$ 个月初已经在围栏中的兔子仍然存在，而且每对在第 $n-2$ 个

月初就存在的兔子将在第 $n-1$ 个月生出一对新兔来，所以有

$$\begin{cases} f(n) = f(n-1) + f(n-2), & n \geqslant 3, n \in Z^+, \\ f(1) = 1, f(2) = 2. \end{cases} \tag{8.4}$$

若令 $f(0) = 1$，则递推方程 8.4 就变成

$$\begin{cases} f(n) = f(n-1) + f(n-2), & n \geqslant 2, n \in Z^+, \\ f(0) = 1, f(1) = 1. \end{cases} \tag{8.5}$$

满足 8.5 式的数列就叫做 Fibonacci 数列，而它的项就叫做 **Fibonacci 数**.

递推方程 8.5 的特征方程是 $x^2 - x - 1 = 0$，特征根是

$$x_1 = \frac{1+\sqrt{5}}{2}, \quad x_2 = \frac{1-\sqrt{5}}{2}.$$

所以通解是

$$f(n) = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

代入初值来确定 c_1 和 c_2，得到方程组

$$\begin{cases} c_1 + c_2 = 1, \\ \dfrac{1+\sqrt{5}}{2}c_1 + \dfrac{1-\sqrt{5}}{2}c_2 = 1. \end{cases}$$

解这个方程组得

$$c_1 = \frac{1}{\sqrt{5}}\,\frac{1+\sqrt{5}}{2}, \quad c_2 = -\frac{1}{\sqrt{5}}\,\frac{1-\sqrt{5}}{2},$$

所以原递推方程的解是

$$f(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}, \; n = 0,1,\cdots.$$

【例 8.2】 用字母 a,b 和 c 组成长为 n 的字，如果要求没有两个 a 相邻，问这样的字有多少个？

解 设 $h(n)$ 是所求的字的个数，$n \geqslant 1$. 长为 1 的没有两个 a 相邻的字有 a,b,c，所以 $h(1) = 3$. 长为 2 的没有两个 a 相邻的字有 ab，

$ac, ba, bb, bc, ca, cb, cc$，所以 $h(2) = 8$.

设 $n \geqslant 3$，如果字中的第一个字母是 a，那么第二个字母只能是 b 或 c，其余的字母可以有 $h(n-2)$ 种方式来选择，因此以 a 开头的字有 $2h(n-2)$ 个. 如果第一个字母是 b，那么这样的字有 $h(n-1)$ 个. 同理以 c 开头的字也有 $h(n-1)$ 个. 由加法法则得

$$\begin{cases} h(n) = 2h(n-1) + 2h(n-2), & n \geqslant 3, \\ h(1) = 3,\ h(2) = 8. \end{cases}$$

该递推方程的特征方程为 $x^2 - 2x - 2 = 0$，特征根是

$$x_1 = 1 + \sqrt{3}, \quad x_2 = 1 - \sqrt{3}.$$

所以通解是

$$h(n) = c_1(1 + \sqrt{3})^n + c_2(1 - \sqrt{3})^n.$$

代入初值来确定 c_1 和 c_2 得

$$\begin{cases} c_1(1 + \sqrt{3}) + c_2(1 - \sqrt{3}) = 3, \\ c_1(1 + \sqrt{3})^2 + c_2(1 - \sqrt{3})^2 = 8. \end{cases}$$

解得

$$c_1 = \frac{2 + \sqrt{3}}{2\sqrt{3}},\ c_2 = \frac{-2 + \sqrt{3}}{2\sqrt{3}}.$$

因此所求的字数是

$$h(n) = \frac{2 + \sqrt{3}}{2\sqrt{3}}(1 + \sqrt{3})^n + \frac{-2 + \sqrt{3}}{2\sqrt{3}}(1 - \sqrt{3})^n, \quad n = 1, 2, \cdots.$$

【例 8.3】 核反应堆中有 α 和 β 两种粒子，每秒钟内 1 个 α 粒子分裂成 3 个 β 粒子，而 1 个 β 粒子分裂成 1 个 α 粒子和 2 个 β 粒子. 若在时刻 $t = 0$ 反应堆中只有 1 个 α 粒子，问 $t = 100$ 秒时反应堆中将有多少个 α 粒子？多少个 β 粒子？共有多少个粒子？

解 设在 t 时刻的 α 粒子数为 $f(t)$，β 粒子数为 $g(t)$. 根据题意

可以列出下面的递推方程组：

$$\begin{cases} g(t) = 3f(t-1) + 2g(t-1), & t \geqslant 1, \quad ① \\ f(t) = g(t-1), & t \geqslant 1, \quad ② \\ g(0) = 0,\ f(0) = 1. \end{cases}$$

由 ② 式得 $f(t-1) = g(t-2)$，代入 ① 式得

$$\begin{cases} g(t) = 2g(t-1) + 3g(t-2), & t \geqslant 2, \quad ③ \\ g(0) = 0,\ g(1) = 3f(0) + 2g(0) = 3. \end{cases}$$

该递推方程的特征方程是 $x^2 - 2x - 3 = 0$，其特征根是 $x_1 = 3$，$x_2 = -1$. 所以该递推方程的通解是

$$g(t) = c_1 3^t + c_2(-1)^t.$$

代入初值 $g(0) = 0, g(1) = 3$ 得

$$\begin{cases} c_1 + c_2 = 0, \\ 3c_1 - c_2 = 3. \end{cases}$$

解得

$$c_1 = \frac{3}{4}, \quad c_2 = -\frac{3}{4}.$$

所以递推方程 ③ 的解是

$$g(t) = \frac{3}{4} \cdot 3^t - \frac{3}{4}(-1)^t.$$

从而求得

$$f(t) = g(t-1) = \frac{3}{4} \cdot 3^{t-1} - \frac{3}{4}(-1)^{t-1},$$

$$\begin{aligned} f(t) + g(t) &= \frac{3}{4} \cdot 3^{t-1} - \frac{3}{4}(-1)^{t-1} + \frac{3}{4} \cdot 3^t - \frac{3}{4}(-1)^t \\ &= 3^t. \end{aligned}$$

因此有

$$f(100) = \frac{3}{4} \cdot 3^{99} - \frac{3}{4} \cdot (-1)^{99} = \frac{3}{4}(3^{99} + 1),$$

$$g(100) = \frac{3}{4} \cdot 3^{100} - \frac{3}{4} \cdot (-1)^{100} = \frac{3}{4}(3^{100} - 1),$$

$$f(100)+g(100)=3^{100}.$$

对于 k 阶常系数线性齐次递推方程，当特征根 $q_1,q_2,\cdots,q_k$ 都不相等的时候，我们已经给出了求解的方法. 但是当 $q_1,q_2,\cdots,q_k$ 中有重根时，这种方法就不适用了. 换句话说，$c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$ 就不是原递推方程的通解了. 因为把 k 个初值代入以后得到 k 个方程，但未知数至多为 $k-1$ 个，可能使得方程组无解. 这说明只有在 $q_1,q_2,\cdots,q_k$ 都线性无关时才能得到递推方程的通解.

为了解决重根的情况，先给出下面的引理.

引理 1 设

$$f_0(x)=x^n-a_1x^{n-1}-\cdots-a_{k-1}x^{n-k+1}-a_kx^{n-k},$$

$\forall i\in Z^+$，令 $f_i(x)=xf'_{i-1}(x)$，其中 $f'_{i-1}(x)$ 是 $f_{i-1}(x)$ 的微商，则

$$f_i(x)=n^ix^n-a_1(n-1)^ix^{n-1}-\cdots-a_k(n-k)^ix^{n-k}.$$

证 对 i 施行归纳.

$i=1$ 时有

$$\begin{aligned}f_1(x)&=xf'_0(x)\\&=x(nx^{n-1}-a_1(n-1)x^{n-2}-\cdots-a_k(n-k)x^{n-k-1})\\&=nx^n-a_1(n-1)x^{n-1}-\cdots-a_k(n-k)x^{n-k}.\end{aligned}$$

命题为真.

假设 i 时命题为真，考虑 $i+1$ 的情况.

$$\begin{aligned}&f_{i+1}(x)=xf'_i(x)\\&=x(n^ix^n-a_1(n-1)^ix^{n-1}-\cdots-a_k(n-k)^ix^{n-k})'\\&=x(n^{i+1}x^{n-1}-a_1(n-1)^{i+1}x^{n-2}-\cdots-a_k(n-k)^{i+1}x^{n-k-1})\\&=n^{i+1}x^n-a_1(n-1)^{i+1}x^{n-1}-\cdots-a_k(n-k)^{i+1}x^{n-k}.\end{aligned}$$

由归纳法引理 1 得证. ▮

引理 2 设 $f_i(x)$ 为引理 1 中的 n 次多项式，若 q 是 $f_i(x)$ 的 e 重根，则 q 是 $f_{i+1}(x)$ 的 $e-1$ 重根.

证 因为 q 是 $f_i(x)$ 的 e 重根，即

$$f_i(x) = (x-q)^e \cdot P(x),$$

其中 $P(x)$ 为 $n-e$ 次多项式且 $x-q$ 不整除 $P(x)$，从而

$$\begin{aligned} f_{i+1}(x) &= xf'_i(x) = x[e(x-q)^{e-1} \cdot P(x) + (x-q)^e P'(x)] \\ &= (x-q)^{e-1}[exP(x) + (x-q)xP'(x)]. \end{aligned}$$

又由于 $x-q$ 不整除 $P(x)$，所以 q 是 $f_{i+1}(x)$ 的 $e-1$ 重根. ∎

定理 8.4 设有 k 阶递推方程

$$H(n) - a_1H(n-1) - \cdots - a_kH(n-k) = 0,\ a_k \neq 0,\ n \geqslant k.$$

若 q 是递推方程的 e 重特征根，则 $q^n, nq^n, \cdots, n^{e-1}q^n$ 都是该递推方程的解且是线性无关的解.

证 因为 q 是递推方程的 e 重特征根，则 q 是

$$f_0(x) = x^n - a_1x^{n-1} - \cdots - a_{k-1}x^{n-k+1} - a_kx^{n-k}$$

的 e 重根. 由引理 2，q 是 $f_1(x)$ 的 $e-1$ 重根，q 是 $f_2(x)$ 的 $e-2$ 重根，…，q 是 $f_{e-1}(x)$ 的根. 又由引理 1 有

$$f_i(x) = n^ix^n - a_1(n-1)^ix^{n-1} - \cdots - a_k(n-k)^ix^{n-k},$$

对 $i = 1,2,\cdots,e-1$，将 $x = q$ 代入得

$$n^iq^n - a_1(n-1)^iq^{n-1} - \cdots - a_k(n-k)^iq^{n-k} = 0.$$

这就推出 $n^iq^n (i = 1,2,\cdots,e-1)$ 也是递推方程的解. 从而 $q^n, nq^n, \cdots, n^{e-1}q^n$ 都是递推方程的解. 下面证明这些解是线性无关的.

假若存在常数 $c_1, c_2, \cdots, c_e$ 使得

$$c_1q^n + c_2nq^n + \cdots + c_en^{e-1}q^n = 0.$$

由于 $q \neq 0$，n 是任意正整数，必有 $c_1 = c_2 = \cdots = c_e = 0$. ∎

定理 8.5 设 $q_1, q_2, \cdots, q_t$ 是递推方程

$$H(n) - a_1H(n-1) - \cdots - a_kH(n-k) = 0,\ a_k \neq 0,\ n \geqslant k$$

的不相等的特征根，且 q_i 的重数为 e_i，$i = 1,2,\cdots,t$. 令 $c_{i1}, c_{i2}, \cdots, c_{ie_i}$ 是任意常数，且

$$H_i(n) = (c_{i1} + c_{i2}n + \cdots + c_{ie_i}n^{e_i-1})q_i^n,\ i = 1,2,\cdots,t,$$

则 $H(n) = \sum_{i=1}^{t} H_i(n)$ 是递推方程的通解.

证 由定理 8.4 和 8.2，$\forall i = 1,2,\cdots,t$，$H_i(n)$ 是递推方程的解. 又由定理 8.2，$H(n) = \sum_{i=1}^{t} H_i(n)$ 也是递推方程的解. 下面证明 $H(n)$ 是通解.

设 $h(n)$ 是递推方程的任意一个解，且由初值 $h(0)=b_0$，$h(1)=b_1$，$\cdots$，$h(k-1)=b_{k-1}$ 唯一地确定，从而得到方程组

$$
\begin{cases}
c_{11}+\cdots+c_{1e_1}+c_{21}+\cdots+c_{2e_2}+\cdots+c_{t1}+\cdots+c_{te_t}=b_0, \\
c_{11}q_1+\cdots+c_{1e_1}q_1+c_{21}q_2+\cdots+c_{2e_2}q_2+\cdots+c_{t1}q_t+\cdots+c_{te_t}q_t=b_1, \\
c_{11}q_1^2+\cdots+c_{1e_1}2^{e_1-1}q_1^2+c_{21}q_2^2+\cdots+c_{2e_2}2^{e_2-1}q_2^2+\cdots+c_{t1}q_t^2+\cdots+c_{te_t}2^{e_t-1}q_t^2=b_2, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
c_{11}q_1^{k-1}+\cdots+c_{1e_1}(k-1)^{e_1-1}q_1^{k-1}+c_{21}q_2^{k-1}+\cdots+c_{2e_2}(k-1)^{e_2-1}q_2^{k-1} \\
\qquad +\cdots+c_{t1}q_t^{k-1}+\cdots+c_{te_t}(k-1)^{e_t-1}q_t^{k-1}=b_{k-1}.
\end{cases}
$$

该方程组的系数行列式是

$$
\begin{vmatrix}
1 & \cdots & 1 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 \\
q_1 & \cdots & q_1 & q_2 & \cdots & q_2 & \cdots & q_t & \cdots & q_t \\
q_1^2 & \cdots & 2^{e_1-1}q_1^2 & q_2^2 & \cdots & 2^{e_2-1}q_2^2 & \cdots & q_t^2 & \cdots & 2^{e_t-1}q_t^2 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
q_1^{k-1} & \cdots & (k-1)^{e_1-1}q_1^{k-1} & q_2^{k-1} & \cdots & (k-1)^{e_2-1}q_2^{k-1} & \cdots & q_t^{k-1} & \cdots & (k-1)^{e_t-1}q_t^{k-1}
\end{vmatrix}.
$$

这是推广的 Vandermonde 行列式，其值是

$$\prod_{i=1}^{t}(-q_i)\binom{e_i}{2}\prod_{1\leqslant i<j\leqslant t}(q_j-q_i)^{e_je_i}.$$

由于 $q_j \neq q_i (j \neq i)$，所以行列式不为 0，方程组有唯一解，即存在常数 c'_{11}，$\cdots$，c'_{1e_1}，c'_{21}，$\cdots$，c'_{2e_2}，c'_{t1}，$\cdots$，c'_{te_t} 使得

$$h(n) = \sum_{i=1}^{t}(c'_{i1}+c'_{i2}n+\cdots+c'_{ie_i}n^{e_i-1})q_i^n.$$

从而证明 $H(n)$ 是递推方程的通解. ∎

【例 8.4】 求解递推方程

$$\begin{cases} H(n) + H(n-1) - 3H(n-2) - 5H(n-3) \\ \qquad\qquad\qquad\qquad - 2H(n-4) = 0, n \geqslant 4, \\ H(0) = 1, H(1) = 0, H(2) = 1, H(3) = 2. \end{cases}$$

解 该递推方程的特征方程是

$$x^4 + x^3 + 3x^2 - 5x - 2 = 0,$$

它的特征根是 $-1, -1, -1, 2$. 根据定理 8.5，该递推方程的通解是

$$H(n) = c_1(-1)^n + c_2 n(-1)^n + c_3 n^2(-1)^n + c_4 \cdot 2^n.$$

代入初值得到下列方程组

$$\begin{cases} c_1 + c_4 = 1, \\ -c_1 - c_2 - c_3 + 2c_4 = 0, \\ c_1 + 2c_2 + 4c_3 + 4c_4 = 1, \\ -c_1 - 3c_2 - 9c_3 + 8c_4 = 2. \end{cases}$$

解这个方程组得

$$c_1 = \frac{7}{9}, c_2 = -\frac{1}{3}, c_3 = 0, c_4 = \frac{2}{9}.$$

所以原递推方程的解是

$$H(n) = \frac{7}{9}(-1)^n - \frac{1}{3}n(-1)^n + \frac{2}{9} \cdot 2^n.$$

下面考虑常系数线性非齐次递推方程，它的一般形式是

$$\begin{cases} H(n) - a_1 H(n-1) - \cdots - a_k H(n-k) = f(n), \\ \qquad n \geqslant k, a_k \neq 0, f(n) \neq 0. \end{cases} \tag{8.6}$$

先讨论这种递推方程的通解.

定理 8.6 设 $\overline{H(n)}$ 是常系数线性齐次递推方程

$$\begin{cases} H(n) - a_1 H(n-1) - \cdots - a_k H(n-k) = 0, \\ n \geqslant k, a_k \neq 0 \end{cases} \tag{8.7}$$

的通解，$H^*(n)$ 是递推方程 8.6 的一个特解，则

$$H(n) = \overline{H}(n) + H^*(n)$$

是递推方程 8.6 的通解.

证 $H(n)$ 是递推方程 8.6 的解,因为将它代入递推方程的左边得

$$\begin{aligned}
&[\overline{H}(n) + H^*(n)] - a_1[\overline{H}(n-1) + H^*(n-1)] - \cdots \\
&\quad - a_k[\overline{H}(n-k) + H^*(n-k)] \\
&= [\overline{H}(n) - a_1\overline{H}(n-1) - \cdots - a_k\overline{H}(n-k)] \\
&\quad + [H^*(n) - a_1H^*(n-1) - \cdots - a_kH^*(n-k)] \\
&= 0 + f(n) = f(n).
\end{aligned}$$

再证明 $H(n)$ 是通解. 设 $h(n)$ 是递推方程 8.6 的一个解,则有

$$h(n) - a_1h(n-1) - \cdots - a_kh(n-k) = f(n).$$

而

$$H^*(n) - a_1H^*(n-1) - \cdots - a_kH^*(n-k) = f(n).$$

将这两个式子相减得

$$\begin{aligned}
&[h(n) - H^*(n)] - a_1[h(n-1) - H^*(n-1)] - \cdots \\
&\quad - a_k[h(n-k) - H^*(n-k)] = 0.
\end{aligned}$$

这说明 $h(n) - H^*(n)$ 是对应齐次递推方程 8.7 的解. 因此 $h(n)$ 是一个齐次解与 $H^*(n)$ 之和,从而证明了 $\overline{H}(n) + H^*(n)$ 是递推方程 8.6 的通解. ∎

根据这个定理,只要找到递推方程 8.6 的一个特解,就可以得到它的通解. 但遗憾的是对于一般的 $f(n)$ 并不存在寻找特解的普遍方法,只能用观察法猜想特解的形式,然后用待定系法的方法来确定系数. 下面分情况讨论.

当 $f(n)$ 是 n 的 t 次多项式时,一般情况下可以设特解 $H^*(n)$ 也是 n 的 t 次多项式,即

$$H^*(n) = P_1n^t + P_2n^{t-1} + \cdots + P_tn + P_{t+1},$$

其中 $P_1, P_2, \cdots, P_{t+1}$ 是待定系数.

【例 8.5】 求解递推方程

$$H(n)+5H(n-1)+6H(n-2)=3n^2$$

的一个特解.

解 假设 $H^*(n)=P_1n^2+P_2n+P_3$,代入原递推方程得

$$P_1n^2+P_2n+P_3+5[P_1(n-1)^2+P_2(n-1)+P_3]$$
$$+6[P_1(n-2)^2+P_2(n-2)+P_3]=3n^2,$$

化简左边得

$$12P_1n^2+(-34P_1+12P_2)n+(29P_1-17P_2+12P_3)=3n^2,$$

从而有

$$\begin{cases}12P_1=3,\\-34P_1+12P_2=0,\\29P_1-17P_2+12P_3=0.\end{cases}$$

解得 $P_1=\dfrac{1}{4}$, $P_2=\dfrac{17}{24}$, $P_3=\dfrac{115}{288}$. 所求的特解是

$$H^*(n)=\frac{1}{4}n^2+\frac{17}{24}n+\frac{115}{288}.$$

【例 8.6】 求解递推方程

$$H(n)-H(n-1)=7n$$

的特解.

解 如果我们设

$$H^*(n)=P_1n+P_2,$$

代入原递推方程得

$$(P_1n+P_2)-[P_1(n-1)+P_2]=7n,$$

化简得

$$P_1=7n.$$

从上式解不出 P_1 和 P_2. 这是因为当原递推方程的特征根是 1 时,如果所设的特解中 n 的最高次幂的次数与 $f(n)$ 的次数一样,代入原递推方程后,等式左边的 n 的最高次幂就会消去. 因此等式左边的多项

式比右边的多项式的次数低.为此,在设特解时要将 n 的最高次幂提高,并且可以不设常数项.这里我们设

$$H^*(n) = P_1n^2 + P_2n,$$

代入原递推方程后得

$$(P_1n^2 + P_2n) - [P_1(n-1)^2 + P_2(n-1)] = 7n,$$

化简上式得

$$2P_1n + P_2 - P_1 = 7n.$$

解得 $P_1 = P_2 = \frac{7}{2}$,因此所求的特解是

$$H^*(n) = \frac{7}{2}n(n+1).$$

【例 8.7】 Hanoi 塔问题.

如图 8.1,n 个圆盘按从大到小的顺序依次套在柱 A 上.每次从一根柱子只能搬动一个圆盘到另一根柱子上.如果在搬动过程中不允许大圆盘放在小圆盘的上面,请设计一个计算机算法将所有的圆盘从柱 A 移到柱 B,并分析算法的时间复杂性.

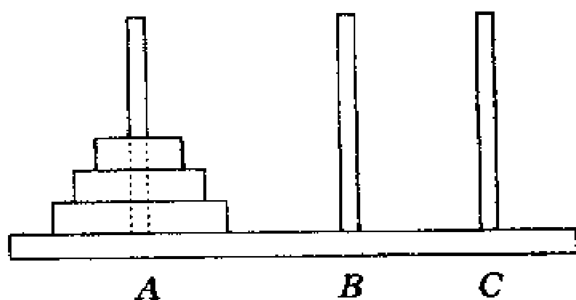


图 8.1

解 这是一个典型的递归算法.令 MOVE(n,X,Y) 表示将 n 个盘子从柱 X 移到柱 Y.则算法 MOVE(n,A,B) 可表示为:

1. 初始化,$S \leftarrow \{A,B,C\}$;
2. MOVE (n,A,B).

```
MOVE (n,X,Y);
1. if n = 1 then TAKE(X,Y)
2. else
   {从 S - {X,Y} 中取 Z;
```

```
        MOVE (n - 1, X, Z);
        TAKE (X,Y);
        MOVE (n - 1, Z, Y).
    }
```

其中 TAKE(X,Y) 表示从柱 X 拿一个盘子到柱 Y.

下面考虑算法的复杂性. 该算法的主要运算是移动盘. 设 n 个盘子的移动次数为 $H(n)$,根据算法列出递推方程如下:

$$\begin{cases} H(n) = 2H(n-1) + 1, & n \geqslant 2, \\ H(1) = 1. \end{cases}$$

这是一个常系数线性非齐次的递推方程,它的齐次通解为 $c2^n$. 设它的特解为 P,代入原方程得

$$P - 2P = 1,$$

解得 $P = -1$,从而得到原方程的通解是 $c \cdot 2^n - 1$,代入初值得

$$2c - 1 = 1,$$

解得 $c = 1$,$H(n) = 2^n - 1$. 这说明该算法的移动次数是 $2^n - 1$,它的时间复杂性是 $O(2^n)$.

下面考虑 $f(n)$ 是指数函数的情况.

若 $f(n) = \alpha \cdot \beta^n$,其中 α 和 β 是给定常数,则递推方程 8.6 的特解可以如下设定:

若 β 不是递推方程 8.7 的特征根,则令 $H^*(n) = P \cdot \beta^n$;若 β 是递推方程 8.7 的 e 重特征根,则令 $H^*(n) = Pn^e\beta^n$. 这里的 P 都是待定系数.

【例 8.8】 求解递推方程

$$\begin{cases} H(n) + 5H(n-1) + 6H(n-2) = 42 \cdot 4^n, \\ H(0) = 0,\ H(1) = 0. \end{cases}$$

解 该递推方程的齐次通解为 $c_1(-2)^n + c_2(-3)^n$. 设它的特解为 $P \cdot 4^n$,代入原方程得

$$P \cdot 4^n + 5P \cdot 4^{n-1} + 6P \cdot 4^{n-2} = 42 \cdot 4^n,$$

解得 $P=16$，从而得到通解

$$H(n)=c_1(-2)^n+c_2(-3)^n+16\cdot 4^n.$$

代入初值得到方程组

$$\begin{cases}c_1+c_2+16=0,\\ c_1(-2)+c_2(-3)+64=0.\end{cases}$$

解得 $c_1=-112$，$c_2=96$. 因此原递推方程的解是

$$H(n)=-112(-2)^n+96(-3)^n+16\cdot 4^n.$$

【例 8.9】 求解递推方程

$$\begin{cases}a_n-4a_{n-1}+4a_{n-2}=2^n,\\ a_0=1,\quad a_1=5.\end{cases}$$

解 该递推方程的齐次通解为 $(c_1+c_2n)2^n$. 由于 2 是对应齐次方程的二重根，因此设特解为 Pn^22^n，代入原递推方程得

$$Pn^22^n-4P(n-1)^22^{n-1}+4P(n-2)^22^{n-2}=2^n,$$

解出 $P=\dfrac{1}{2}$. 从而得到原递推方程的通解

$$a_n=c_12^n+c_2n2^n+\frac{1}{2}n^22^n.$$

代入初值得到方程组

$$\begin{cases}c_1=1,\\ 2c_1+2c_2+1=5.\end{cases}$$

解出 $c_1=1$，$c_2=1$. 因此原递推方程的解是

$$a_n=2^n+n2^n+n^22^{n-1}.$$

§8.2 递推方程的其它解法

除了常系数线性递推方程的公式解法以外，还有一些求解递推方程的方法，如换元法、迭代归纳法、差消法、尝试法等等. 下面分别加以说明.

某些非常系数非线性的递推方程通过换元可以变成常系数线性

递推方程，然后用公式法求解．这种求解方法称作换元法．

【例 8.10】 求解递推方程

$$\begin{cases} a_n^2 = 2a_{n-1}^2 + 1, & a_n > 0, \\ a_0 = 2. \end{cases}$$

解 令 $b_n = a_n^2$，代入原递推方程得

$$\begin{cases} b_n - 2b_{n-1} = 1, \\ b_0 = 4. \end{cases}$$

这是一个常系数线性递推方程，解是 $b_n = 5 \cdot 2^n - 1$，从而得到原递推方程的解 $a_n = \sqrt{5 \cdot 2^n - 1}$.

【例 8.11】 求解递推方程

$$\begin{cases} a_n^2 - 2a_{n-1} = 0, & a_n > 0, \\ a_0 = 4. \end{cases}$$

解 原方程可变形为

$$a_n^2 = 2a_{n-1},$$

取对数得

$$\begin{cases} 2\log_2 a_n = \log_2 2 + \log_2 a_{n-1}, \\ \log_2 a_0 = 2. \end{cases}$$

令 $b_n = \log_2 a_n$，代入方程得

$$\begin{cases} b_n = \dfrac{1}{2} b_{n-1} + \dfrac{1}{2}, \\ b_0 = 2. \end{cases}$$

解得 $b_n = \left(\dfrac{1}{2}\right)^n + 1$，从而得到原递推方程的解

$$a_n = 2^{b_n} = 2^{\left(\frac{1}{2}\right)^n + 1}.$$

【例 8.12】 求解递推方程

$$\begin{cases} H(n) = H(n/2) + 2, & n = 2^k,\ k = 1, 2, \cdots, \\ H(1) = 1. \end{cases}$$

解 将 $n=2^k$ 代入原递推方程得

$$\begin{cases}H(2^k)=H(2^{k-1})+2,\\H(2^0)=1.\end{cases}$$

令 $T(k)=H(2^k)$,得

$$\begin{cases}T(k)-T(k-1)=2,\\T(0)=1.\end{cases}$$

解得 $T(k)=2k+1$,即 $H(2^k)=2k+1$. 由 $k=\log_2 n$ 可得

$$H(n)=2\log_2 n+1.$$

【例 8.13】 确定以下递推方程的解的阶.

$$T(n)=2T(4n^{\frac{1}{2}})+\log_2 n. \qquad ①$$

解 为把方程 ① 变换成常系数线性递推方程,必须选择一个适当的 k,使得方程具有下述形式

$$H(k)=2H(k-1)+f(k), \qquad ②$$

令 n_k 表示与给定的 k 相对应的 n,由式 ① 与式 ② 有

$$n_{k-1}=4n_k^{\frac{1}{2}}\Rightarrow \log_2 n_{k-1}=2+\frac{1}{2}\log_2 n_k$$

$$\Rightarrow \log_2 n_k-2\log_2 n_{k-1}=-4.$$

令 $m_k=\log_2 n_k$ 得

$$m_k-2m_{k-1}=-4,$$

解得 $m_k=2^k+4$,从而有 $n_k=2^{2^k+4}$,且

$$H(k)=2H(k-1)+\log_2 n_k=2H(k-1)+2^k+4. \qquad ③$$

方程 ③ 的特解设为 $P_1k2^k+P_2$,代入解得

$$P_1=1,\ P_2=-4.$$

所以有

$$H(k)=k2^k+c2^k-4.$$

其中 c 为任意常数. 这就推出

$$T(n_k)=k2^k+c2^k-4,\quad c\text{ 为常数}.$$

因此有

$$T(n) = O(k2^k),$$

而由 $n_k = 2^{2^k+4}$ 知 $k = \log_2(\log_2 n_k - 4)$，从而有

$$T(n) = O(\log_2\log_2 n \cdot \log_2 n).$$

迭代归纳法是求解递推方程的另一种基本方法.它的基本思想是：用迭代的方法推测出递推方程的解，然后用归纳法验证.

【例 8.14】 给定 n 个实数 $a_1, a_2, \cdots, a_n$，可以用多少种不同的方法来构成它们的乘积？这里认为相乘的次序不同也是不同的方法，如 $(a_1 \times a_2) \times a_3$ 与 $a_1 \times (a_2 \times a_3)$ 是不同的方法.

解 令 $h(n)$ 表示这 n 个数构成乘积的方法数.显然有 $h(1) = 1$.假设 $n-1$ 个数 $a_1, a_2, \cdots, a_{n-1}$ 的乘积已经构成，有 $h(n-1)$ 个.任取其中的一个乘积，它是由 $n-2$ 次乘法得到的.对于其中某一次相乘的两个因式，加入 a_n 的方法有 4 种.由加法法则，这种加入 a_n 的方法共 $4(n-2)$ 种.此外，还可以把 a_n 分别乘在整个乘积的左边或右边，因此加入 a_n 的方法数是

$$4(n-2) + 2 = 4n - 6.$$

根据以上的分析可以列出递推方程

$$\begin{cases} h(n) = (4n-6)h(n-1), & n \geqslant 2, \\ h(1) = 1. \end{cases}$$

下面用迭代归纳法求解.

$$\begin{aligned} h(h) &= (4n-6)h(n-1) \\ &= (4n-6)(4n-10)h(n-2) \\ &= (4n-6)(4n-10)(4n-14)h(n-3) \\ &= \cdots \\ &= (4n-6)(4n-10)\cdots 6 \cdot 2 \cdot h(1) \\ &= 2^{n-1}[(2n-3)(2n-5)\cdots 3 \cdot 1] \\ &= 2^{n-1}\frac{(2n-2)!}{(2n-2)(2n-4)\cdots 4 \cdot 2} \end{aligned}$$

$$=\frac{(2n-2)!}{(n-1)!}=(n-1)!\binom{2n-2}{n-1}, \quad n\geqslant 2.$$

由于当 $n=1$ 时,上式的结果也等于1,与初值一致,因此原递推方程的解是

$$h(n)=(n-1)!\binom{2n-2}{n-1}, \quad n\geqslant 1.$$

这个结果是否正确,要通过归纳法加以验证.

$n=1$ 时显然等式成立.

假设 $n=k$ 时等式也成立,则

$$\begin{aligned}h(k+1)&=[4(k+1)-6]h(k)\\&=(4k-2)\cdot(k-1)!\binom{2k-2}{k-1}\\&=2(2k-1)(k-1)!\binom{2k-2}{k-1}\\&=\frac{2k\cdot(2k-1)!}{k!}=k!\binom{2k}{k}.\end{aligned}$$

由归纳法可以知道构成乘积的方法数是 $(n-1)!\binom{2n-2}{n-1}$.

【例 8.15】 求解递推方程

$$\begin{cases}D_n=(n-1)(D_{n-1}+D_{n-2}),\\D_1=0,\ D_2=1.\end{cases}$$

解 由递推方程得

$$D_n-nD_{n-1}=-[D_{n-1}-(n-1)D_{n-2}],$$
$$D_{n-1}-(n-1)D_{n-2}=-[D_{n-2}-(n-2)D_{n-3}],$$
$$D_{n-2}-(n-2)D_{n-3}=-[D_{n-3}-(n-3)D_{n-4}],$$
$$\cdots$$
$$D_3-3D_2=-[D_2-2D_1].$$

把后面的式子依次代入前一个等式得

$$
\begin{aligned}
D_n - nD_{n-1} &= (-1)^2[D_{n-2} - (n-2)D_{n-3}] \\
&= (-1)^3[D_{n-3} - (n-3)D_{n-4}] \\
&= \cdots \\
&= (-1)^{n-2}[D_2 - 2D_1].
\end{aligned}
$$

将初值代入得递推方程

$$
\begin{cases}
D_n - nD_{n-1} = (-1)^n, & n \geqslant 2. \\
D_1 = 0.
\end{cases}
$$

对以上方程做迭代得

$$
\begin{aligned}
D_n &= n[(n-1)D_{n-2} + (-1)^{n-1}] + (-1)^n \\
&= n(n-1)D_{n-2} + n(-1)^{n-1} + (-1)^n \\
&= n(n-1)[(n-2)D_{n-3} + (-1)^{n-2}] + n(-1)^{n-1} + (-1)^n \\
&= \cdots \\
&= n(n-1)\cdots \cdot 2 \cdot D_1 + n(n-1)\cdots \cdot 3 \cdot (-1)^2 + n(n-1) \\
&\quad \cdots \cdot 4 \cdot (-1)^3 + \cdots + n(-1)^{n-1} + (-1)^n \\
&= n!\left[(-1)^2\frac{1}{2!} + (-1)^3\frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}\right] \\
&= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n\frac{1}{n!}\right].
\end{aligned}
$$

下面用归纳法验证.

易见 $D_1 = 1!\left[1 - \frac{1}{1!}\right] = 0$, $D_2 = 2!\left[1 - \frac{1}{1!} + \frac{1}{2!}\right] = 1$.

假设对一切 $k < n$ 结论为真,则

$$
\begin{aligned}
D_n &= (n-1)(D_{n-1} + D_{n-2}) \\
&= (n-1)(n-1)!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1}\frac{1}{(n-1)!}\right] \\
&\quad + (n-1)(n-2)!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-2}\frac{1}{(n-2)!}\right] \\
&= n(n-1)!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-1}\frac{1}{(n-1)!}\right]
\end{aligned}
$$

$$
\begin{aligned}
&-(n-1)!\left[1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^{n-1}\frac{1}{(n-1)!}\right]\\
&+(n-1)!\left[1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^{n-2}\frac{1}{(n-2)!}\right]\\
=&n!\left[1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^{n-1}\frac{1}{(n-1)!}\right]\\
&+(-1)^n\frac{(n-1)!}{(n-1)!}\\
=&n!\left[1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!}\right].
\end{aligned}
$$

由归纳法原递推方程的解是

$$D_n=n!\left[1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!}\right].$$

下面考虑差消法，请看例 8.16.

【例 8.16】 求解递推方程

$$\begin{cases}T(n)=\dfrac{2}{n}\displaystyle\sum_{i=1}^{n-1}T(i)+n+1 \quad n\geqslant 2,\\ T(1)=0.\end{cases} \quad ①$$

由式 ① 得

$$nT(n)=2\sum_{i=1}^{n-1}T(i)+n^2+n. \quad ②$$

将式 ② 中的 n 用 $n-1$ 代入得

$$(n-1)T(n-1)=2\sum_{i=1}^{n-2}T(i)+(n-1)^2+n-1. \quad ③$$

由式 ② 减去式 ③ 得

$$nT(n)-(n-1)T(n-1)=2T(n-1)+2n,$$

化简得

$$nT(n)=(n+1)T(n-1)+2n,$$

$$\frac{T(n)}{n+1}=\frac{T(n-1)}{n}+\frac{2}{n+1}.$$

由迭代法得

$$\begin{aligned}\frac{T(n)}{n+1} &= \frac{2}{n+1} + \frac{2}{n} + \frac{T(n-2)}{n-1} \\ &= \cdots \\ &= \frac{2}{n+1} + \frac{2}{n} + \cdots + \frac{2}{3} + \frac{T(1)}{2} \\ &= 2\left(\frac{1}{n+1} + \frac{1}{n} + \cdots + \frac{1}{3}\right).\end{aligned}$$

因此

$$T(n) = 2(n+1)\left(\frac{1}{n+1} + \frac{1}{n} + \cdots + \frac{1}{3}\right).$$

我们估计一下 $T(n)$ 的阶. 由于

$$\sum_{i=3}^{n+1} \frac{1}{i} < \int_{2}^{n+1} \frac{1}{x} \mathrm{d}x$$

(参见图 8.2), 即

$$\sum_{i=3}^{n+1} \frac{1}{i} = O(\log n),$$

所以 $T(n) = O(n\log n)$①.

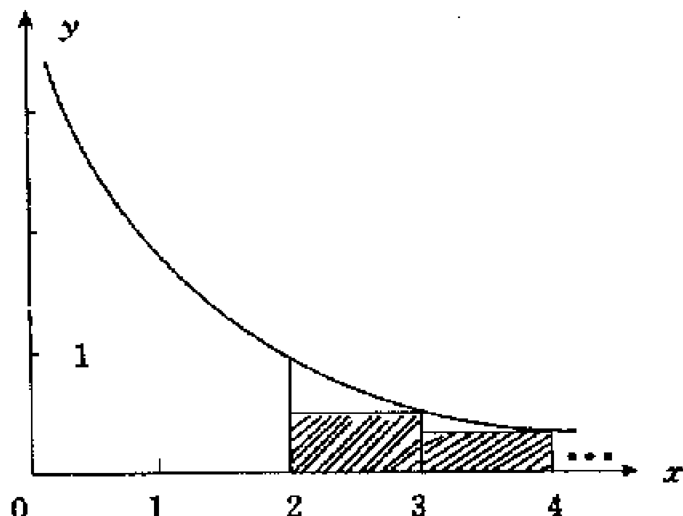


图 8.2

例 8.16 中的递推方程称为全部历史递推方程, 由于 $T(n)$ 是由 $T(0), T(1), \cdots, T(n-1)$ 等所有的项确定. 通过差消法消去大多数项, 只保留后面的几项将递推方程化简, 然后用迭代归纳法或换元法求解.

最后谈谈尝试法. 所谓尝试法就是根据递推方程中的函数形式, 先猜想出递推方程的解的函数形式, 如常数、一次函数、二次函数、指数函数、对数函数 …, 然后代入方程验证. 如果满足方程, 则它就是递推方程的解. 这种解法在算法分析中是经常用到的. 由递归算法所

① $\log n$ 就是 $\log_2 n$

得到的递推方程往往比较复杂，许多方程至今还得不到精确解. 但对于算法分析来说，我们只关心解的阶，这时不妨用尝试法试一试.

先看例 8.16 的递推方程

$$T(n) = \frac{2}{n}\sum_{i=1}^{n-1}T(i) + n + 1, \quad n \geqslant 2.$$

为估计$T(n)$的阶，先猜想$T(n)$的函数形式然后代入原方程验证. 首先假设 $T(n) = c$，c 是常数，代入递推方程得

$$c = 2c + n + 1 - \frac{2c}{n},$$

等式左边为常数，右边为函数，显然是不成立的. 再假设 $T(n) = cn$，代入递推方程得

$$\begin{aligned} cn &= \frac{2}{n}\sum_{i=1}^{n-1}ci + n + 1 \\ &= c(n-1) + n + 1 \\ &= (c+1)n - c + 1. \end{aligned}$$

等式也不成立. 再令 $T(n) = cn^2$，代入递推方程得

$$\begin{aligned} cn^2 &= \frac{2}{n}\sum_{i=1}^{n-1}ci^2 + n + 1 \\ &= \frac{2}{n}\left[c\frac{n^3}{3} + O(n^2)\right] + n + 1 \\ &= \frac{2}{3}cn^2 + O(n). \end{aligned}$$

等式右端的增长率小于左端的增长率. $T(n)$ 的阶应界于 cn 和 cn^2 之间. 令 $T(n) = cn\log n$，代入原递推方程得

$$\begin{aligned} cn\log n &= \frac{2c}{n}\sum_{i=1}^{n-1}i\log i + n + 1 \\ &= \frac{2c}{n}\left[\frac{n^2}{2}\log n - \frac{n^2}{4\ln 2} + O(n\log n)\right] + n + 1 \\ &= cn\log n + \left(1 - \frac{c}{2\ln 2}\right)n + O(\log n). \end{aligned}$$

令 $c = 2\ln 2$，则方程右端与左端的增长率是一致的，因此解得 $T(n)$ 的阶为

$$T(n) = O(n\log n).$$

例 8.16 的递推方程实际上是快速排序算法在做平均状况下的时间复杂性分析时所得到的递推方程. 设被排序的序列为 x_f, $x_{f+1}, \cdots, x_l$. 将快速排序算法记为 Quicksort(f,l)，描述如下：

Quicksort(f,l)

1. 如果 $f \geqslant l$，则算法结束.
2. $i \leftarrow f + 1$.
3. 当 $x_i \leqslant x_f$ 时做 $i \leftarrow i + 1$（从左到右找到大于 x_f 的第一个数 x_i）.
4. $j \leftarrow l$.
5. 当 $x_j \geqslant x_f$ 时做 $j \leftarrow j - 1$（从右到左找到小于 x_f 的第一个数 x_j）.
6. 当 $i < j$ 时做

    $x_i \leftrightarrow x_j$（x_i 和 x_j 交换）.

    $i \leftarrow i + 1$.

    当 $x_i \leqslant x_f$ 时做 $i \leftarrow i + 1$.

    $j \leftarrow j - 1$.

    当 $x_j \geqslant x_f$ 时做 $j \leftarrow j - 1$.

7. $x_f \leftrightarrow x_j$（把 x_f 放好，原来的序列划分成两个子序列）.
8. Quicksort$(f, j - 1)$.
9. Quicksort$(j + 1, l)$.

图 8.3 给出了用 Quicksort 算法排序的一个实例. 输入为 13 个数的序列. 图中只是给出了算法从步 1 到步 7 的执行结果.

下面分析一下 Quicksort 算法在平均状况下的时间复杂性. 到第 7 步结束时，$x_{f+1}, \cdots, x_{s-1}$ 分别与 x_f 比较了一次，$x_{s+2}, \cdots, x_l$ 也分别与 x_f 比较了一次，而 x_s, x_{s+1} 各与 x_f 比较了两次. 这 n 个数共比较了

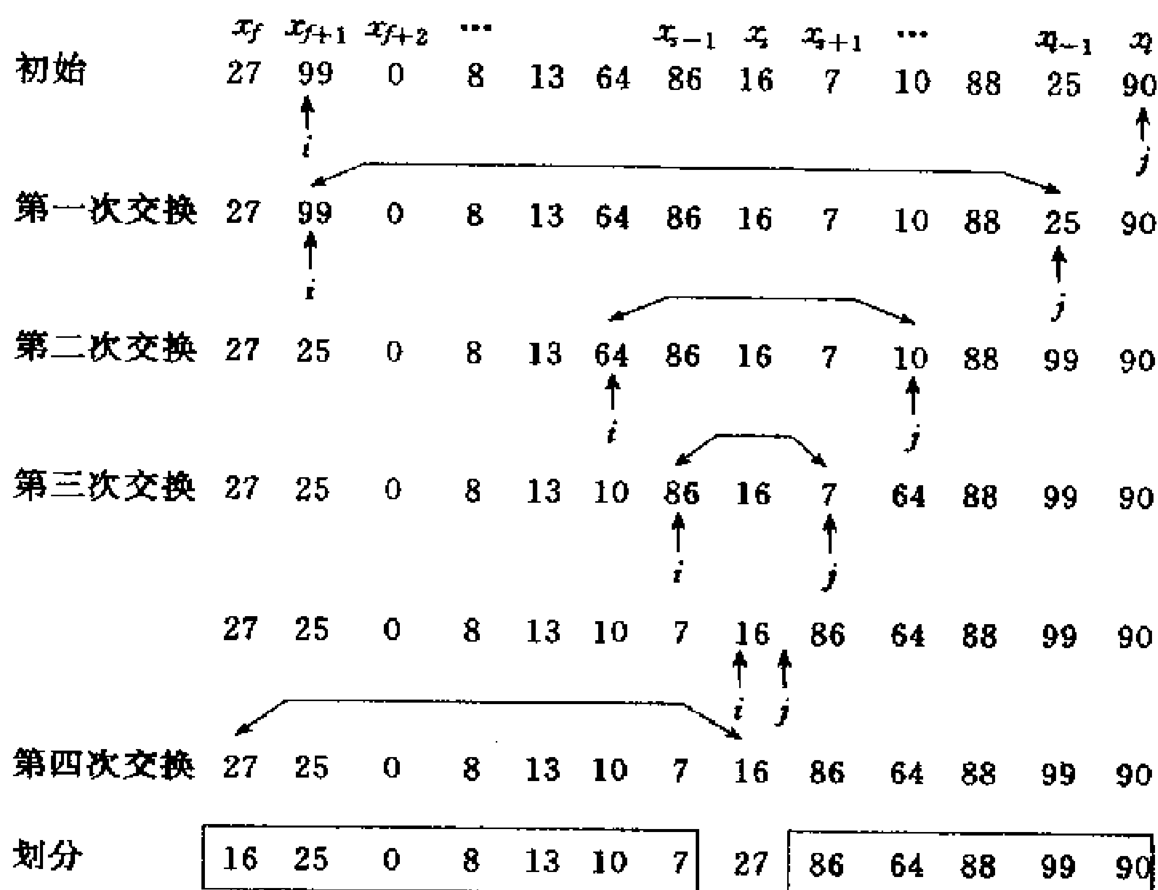


图 8.3

$n+1$ 次. 令 c_n 表示对 n 个数进行快速排序时所用的平均比较次数,P_s 是 x_f 为序列 $x_f,\cdots,x_l$ 中第 s 个最小数的概率. 如果假设当 $s=1,2,\cdots,n$ 时这个概率都相等,即 $P_s=\dfrac{1}{n}$,$s=1,2,\cdots,n$,则有

$$
\begin{aligned}
c_n &= \sum_{s=1}^{n}\frac{1}{n}(n+1+c_{s-1}+c_{n-s}) \\
&= \frac{1}{n}\sum_{s=1}^{n}(c_{s-1}+c_{n-s})+n+1 \\
&= \frac{2}{n}(c_1+c_2+\cdots+c_{n-1})+n+1 \qquad (c_0=0) \\
&= \frac{2}{n}\sum_{s=1}^{n-1}c_s+n+1.
\end{aligned}
$$

就得到例 8.16 的递推方程，故 $c_n = O(n\log n)$.

【例 8.17】 求解递推方程

$$\begin{cases} H(n) = H\left(\frac{n}{r}\right) + H\left(\frac{3}{4}n\right) + cn, & r,c \text{ 为常数}, r > 1, n > n_0, \\ H(n) = cn, & n \leqslant n_0. \end{cases}$$

解 观察到该递推方程是线性的，很可能它的解是如下形式：

$$H(n) = k(r)cn,$$

其中 $k(r)$ 是 r 的函数，代入原递推方程得

$$\begin{aligned} k(r)cn &= k(r) \cdot c\,\frac{n}{r} + k(r) \cdot c\,\frac{3}{4}n + cn \\ &= k(r) \cdot cn\left[\frac{1}{r} + \frac{3}{4} + \frac{1}{k(r)}\right], \end{aligned}$$

从而有

$$\frac{1}{r} + \frac{3}{4} + \frac{1}{k(r)} = 1.$$

解得

$$k(r) = \frac{4r}{r-4}.$$

因此得到

$$H(n) = \frac{4r}{r-4}cn, \qquad n > n_0.$$

经代入原递推方程验证，解是

$$H(n) = \begin{cases} \frac{4r}{r-4}cn, & n > n_0, \\ cn, & n \leqslant n_0. \end{cases}$$

最后我们考察一个分治法的例子. 设 n 表示输入规模，$\frac{n}{b}$ 表示将这个问题划分成 a 个子问题后每个子问题的输入规模，其中 a，b 为常数. $d(n)$ 表示在分解或综合子问题而得到整个问题的解时所花费的时间，则整个问题的时间复杂性函数满足

$$\begin{cases} T(n) = aT\left(\dfrac{n}{b}\right) + d(n), \\ T(1) = 1. \end{cases}$$

由迭代可得

$$\begin{aligned} T(n) &= a^2T(n/b^2) + ad(n/b) + d(n) \\ &= \cdots \\ &= a^k + \sum_{i=0}^{k-1} a^i d(n/b^i). \end{aligned}$$

设 $n = b^k$,则 $k = \log_b n$,即

$$a^k = a^{\log_b n} = n^{\log_b a}.$$

当 $d(n)$ 为常数时,有

$$T(n) = \begin{cases} O(n^{\log_b a}), & a \neq 1, \\ O(\log n), & a = 1. \end{cases}$$

当 $d(n) = cn$,c 为常数时,则

$$\sum_{i=0}^{k-1} a^i d(n/b^i) = \sum_{i=0}^{k-1} a^i (cn/b^i) = cn \sum_{i=0}^{k-1} \left(\frac{a}{b}\right)^i.$$

若 $a < b$,则 $cn \sum_{i=0}^{k-1} \left(\frac{a}{b}\right)^i = O(n)$,那么有

$$T(n) = n^{\log_b a} + O(n) = O(n).$$

若 $a = b$,则 $cn \sum_{i=0}^{k-1} \left(\frac{a}{b}\right)^i = cnk = cn\log_b n$,那么有

$$T(n) = n^{\log_b a} + cn\log_b n = O(n\log n).$$

若 $a > b$,则 $cn \sum_{i=0}^{k-1} \left(\frac{a}{b}\right)^i = cn \dfrac{\left(\frac{a}{b}\right)^k - 1}{\frac{a}{b} - 1} = O(n^{\log_b a})$,从而有

$$T(n) = n^{\log_b a} + O(n^{\log_b a}) = O(n^{\log_b a}).$$

综上所述得

$$T(n) = \begin{cases} O(n), & a < b, \\ O(n\log n), & a = b, \\ O(n^{\log_b a}), & a > b. \end{cases}$$

§8.3 生成函数的定义和性质

生成函数也叫做母函数或发生函数. 利用生成函数可以求解组合计数问题.

定义 8.5 设 $a_0, a_1, \cdots, a_n, \cdots$，是一个数列，做形式幂级数

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots,$$

称 $A(x)$ 是数列 $a_0, a_1, \cdots$ 的**生成函数**，

为了书写的方便，我们将数列 $a_0, a_1, \cdots, a_n, \cdots$ 记作$\{a_n\}$.

【例 8.18】 设 $a_n = \binom{m}{n}$，m 为正整数，求数列$\{a_n\}$的生成函数 $A(x)$.

解 $A(x) = \sum_{n=0}^{\infty} \binom{m}{n} x^n = \sum_{n=0}^{m} \binom{m}{n} x^n = (1 + x)^m.$

这恰好是二项式定理的结果.

下面考虑符号$\binom{r}{n}$，先给出定义.

定义 8.6 对任何实数 r 和整数 n 有

$$\binom{r}{n} = \begin{cases} 0, & n < 0, \\ 1, & n = 0, \\ \dfrac{r(r-1)\cdots(r-n+1)}{n!}, & n > 0. \end{cases}$$

例如

$$\binom{\frac{7}{2}}{5} = \frac{\frac{7}{2} \times \frac{5}{2} \times \frac{3}{2} \times \frac{1}{2} \times \left(-\frac{1}{2}\right)}{5 \times 4 \times 3 \times 2 \times 1} = -\frac{7}{256},$$

$$\binom{-\frac{1}{2}}{0}=1,$$

$$\binom{\frac{6}{7}}{-1}=0.$$

以上定义的$\binom{r}{n}$已经失去了组合意义，只是一个记号，称为**牛顿二项式系数**.

定理 8.7 （牛顿二项式定理）设α是一个实数，则对一切x和y满足$\left|\frac{x}{y}\right|<1$有

$$(x+y)^{\alpha}=\sum_{n=0}^{\infty}\binom{\alpha}{n}x^{n}y^{\alpha-n},$$

其中$\binom{\alpha}{n}=\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$.

关于牛顿二项式定理的证明在一般的数学分析书中都可以找到，这里不再赘述.

当$\alpha=m$（m为正整数）时，如果$n>m$，则$\binom{m}{n}=0$，这时牛顿二项式定理就变成

$$(x+y)^{m}=\sum_{n=0}^{m}\binom{m}{n}x^{n}y^{m-n}.$$

这就是二项式定理，所以牛顿二项式定理是二项式定理的推广，二项式定理是牛顿二项式定理的特例.

当$\alpha=-m$（m为正整数）时，有

$$\binom{\alpha}{n}=\binom{-m}{n}=\frac{(-m)(-m-1)\cdots(-m-n+1)}{n!}$$

$$=\frac{(-1)^{n}m(m+1)\cdots(m+n-1)}{n!}$$

$$= (-1)^n \binom{m+n-1}{n}.$$

所以有

$$(1+z)^{-m} = \frac{1}{(1+z)^m} = \sum_{n=0}^{\infty} (-1)^n \binom{m+n-1}{n} z^n,\ |z| < 1. \tag{8.8}$$

【例8.19】 设α是一个实数,$a_n = \binom{\alpha}{n}$,则数列$\{a_n\}$的生成函数是

$$A(x) = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n = (1+x)^\alpha.$$

而数列$\left\{\binom{m+n-1}{n}\right\}$的生成函数是

$$B(x) = \sum_{n=0}^{\infty} \binom{m+n-1}{n} x^n = \frac{1}{(1-x)^m}. \tag{8.9}$$

特别地,当$m=1$时有

$$B(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x};$$

当$m=2$时有

$$B(x) = \sum_{n=0}^{\infty} \binom{n+1}{1} x^n = \sum_{n=0}^{\infty} (n+1) x^n = \frac{1}{(1-x)^2}.$$

用$-x$代入8.9式中的x得

$$\sum_{n=0}^{\infty} (-1)^n \binom{m+n-1}{n} x^n = \frac{1}{(1+x)^m}.$$

当$m=1$时有

$$\sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}.$$

生成函数作为形式幂级数,它的加法、减法、乘法、除法以及微商、积分都遵从幂级数的运算规则.下面给出生成函数的一些性质.

设数列$\{a_n\}$, $\{b_n\}$, $\{c_n\}$的生成函数分别是$A(x)$, $B(x)$和

$C(x)$.

1. 若 $b_n = \alpha a_n$，α 为常数，则 $B(x) = \alpha A(x)$.

证 $B(x) = \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \alpha a_n x^n = \alpha \sum_{n=0}^{\infty} a_n x^n = \alpha A(x)$. ∎

2. 若 $c_n = a_n + b_n$，则 $C(x) = A(x) + B(x)$.

证明留作练习.

3. 若 $c_n = \sum_{i=0}^{n} a_i b_{n-i}$，则 $C(x) = A(x) \cdot B(x)$.

证 $c_0 = a_0 b_0$,

$c_1 x = a_0 b_1 x + a_1 b_0 x$,

$c_2 x^2 = a_0 b_2 x^2 + a_1 b_1 x^2 + a_2 b_0 x^2$,

…………………………………

$c_n x^n = a_0 b_n x^n + a_1 b_{n-1} x^{n-1} + a_2 b_{n-2} x^{n-2} + \cdots + a_n b_0 x^n$,

…………………………………………………………

把以上各式的两边分别相加得

$$C(x) = a_0 B(x) + a_1 x B(x) + a_2 x^2 B(x) + \cdots + a_n x^n B(x) + \cdots$$
$$= A(x) \cdot B(x).$$ ∎

4. 若 $b_n = \begin{cases} 0, & n < l, \\ a_{n-l}, & n \geqslant l, \end{cases}$ 则 $B(x) = x^l \cdot A(x)$.

证 $B(x) = \sum_{n=0}^{\infty} b_n x^n = \sum_{n=l}^{\infty} b_n x^n = \sum_{n=l}^{\infty} a_{n-l} x^n = x^l \sum_{n=l}^{\infty} a_{n-l} x^{n-l}$

$= x^l \sum_{n=0}^{\infty} a_n x^n = x^l \cdot A(x)$. ∎

5. 若 $b_n = a_{n+l}$，则 $B(x) = \dfrac{A(x) - \sum_{n=0}^{l-1} a_n x^n}{x^l}$.

证明留作练习.

6. 若 $b_n = \sum_{i=0}^{n} a_i$，则 $B(x) = \dfrac{A(x)}{1-x}$.

证 $b_0 = a_0$,

$b_1 x = a_0 x + a_1 x$,

$b_2 x^2 = a_0 x^2 + a_1 x^2 + a_2 x^2$,

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$b_n x^n = a_0 x^n + a_1 x^n + a_2 x^n + \cdots + a_n x^n$,

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

把以上各式的两边分别相加得

$$\begin{aligned}B(x) &= a_0(1 + x + x^2 + \cdots) + a_1 x(1 + x + x^2 + \cdots) \\ &\quad + a_2 x^2(1 + x + x^2 + \cdots) + \cdots \\ &= (a_0 + a_1 x + a_2 x^2 + \cdots)(1 + x + x^2 + \cdots) \\ &= \frac{A(x)}{1 - x}.\end{aligned}$$

∎

7. 若 $b_n = \sum_{i=n}^{\infty} a_i$，且 $A(1) = \sum_{n=0}^{\infty} a_n$ 收敛，则

$$B(x) = \frac{A(1) - xA(x)}{1 - x}.$$

证 因为 $A(1) = \sum_{n=0}^{\infty} a_n$ 收敛，所以 $b_n = \sum_{i=n}^{\infty} a_i$ 是存在的.

$$\begin{aligned}
b_0 &= a_0 + a_1 + a_2 + \cdots = A(1) \\
b_1 x &= a_1 x + a_2 x + \cdots = [A(1) - a_0]x \\
b_2 x^2 &= a_2 x^2 + \cdots = [A(1) - a_0 - a_1]x^2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
b_n x^n &= a_n x^n + \cdots = [A(1) - a_0 - \cdots - a_{n-1}]x^n \\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

把以上各式的两边分别相加得

$$\begin{aligned}B(x) &= A(1) + [A(1) - a_0]x + [A(1) - a_0 - a_1]x^2 + \cdots \\ &\quad + [A(1) - a_0 - a_1 - \cdots - a_{n-1}]x^n + \cdots \\ &= A(1)(1 + x + x^2 + \cdots) - a_0 x(1 + x + x^2 + \cdots)\end{aligned}$$

$$-a_1x^2(1+x+x^2+\cdots)-\cdots$$

$$=[A(1)-x(a_0+a_1x+\cdots)]\cdot(1+x+x^2+\cdots)$$

$$=\frac{A(1)-xA(x)}{1-x}.$$ ∎

8. 若 $b_n=\alpha^n a_n$，α 为常数，则 $B(x)=A(\alpha x)$.

证明留作练习.

9. 若 $b_n=na_n$，则 $B(x)=xA'(x)$，其中 $A'(x)$ 为 $A(x)$ 的微商.

证 由 $A(x)=\sum\limits_{n=0}^{\infty}a_nx^n$ 得

$$A'(x)=\sum_{n=1}^{\infty}na_nx^{n-1},$$

从而

$$xA'(x)=\sum_{n=1}^{\infty}na_nx^n=\sum_{n=0}^{\infty}na_nx^n=\sum_{n=0}^{\infty}b_nx^n=B(x).$$ ∎

10. 若 $b_n=\dfrac{a_n}{n+1}$，则 $B(x)=\dfrac{1}{x}\displaystyle\int_0^x A(x)\mathrm{d}x$.

证明留作练习.

【例 8.20】 求数列$\{a_n\}$的生成函数 $A(x)$.

(1) $a_n=7.3^n$;

(2) $a_n=n(n+1)$;

(3) $a_n=\begin{cases}0, & n=0,1,2,\\(-1)^n, & n\geqslant 3.\end{cases}$

解 (1) 设 $b_n=1$，则$\{b_n\}$的生成函数为$\dfrac{1}{1-x}$，令

$$c_n=3^n=3^n\cdot b^n,$$

由性质 8 得到$\{c_n\}$的生成函数是

$$C(x)=\frac{1}{1-3x}.$$

而 $a_n=7\cdot c_n$，再由性质 1 可得$\{a_n\}$的生成函数

$$A(x)=\frac{7}{1-3x}.$$

(2) 设 $A(x)=\sum_{n=0}^{\infty}a_n x^n=\sum_{n=0}^{\infty}n(n+1)x^n$.

对上式两边积分得

$$\int_0^x A(x)\mathrm{d}x=\sum_{n=0}^{\infty}\int_0^x n(n+1)x^n\mathrm{d}x=\sum_{n=0}^{\infty}nx^{n+1}=x\sum_{n=0}^{\infty}nx^n.$$

$\{1\}$ 的生成函数是$\frac{1}{1-x}$,由性质 9 可知$\{n\}$ 的生成函数是

$$x\left(\frac{1}{1-x}\right)'=\frac{x}{(1-x)^2}.$$

所以有

$$\int_0^x A(x)\mathrm{d}x=\frac{x^2}{(1-x)^2}.$$

对上式两边微商得

$$A(x)=\frac{2x}{(1-x)^3}.$$

(3) $A(x)=\sum_{n=0}^{\infty}a_n x^n=\sum_{n=3}^{\infty}(-1)^n x^n=x^3\sum_{n=3}^{\infty}(-1)^n x^{n-3}$

$$=-x^3\sum_{n=0}^{\infty}(-1)^n x^n=\frac{-x^3}{1+x}.$$

【例 8.21】 已知数列$\{a_n\}$ 的生成函数是

$$A(x)=\frac{2+3x-6x^2}{1-2x},$$

求 a_n.

解 用部分分式的方法得

$$A(x)=\frac{2+3x-6x^2}{1-2x}=\frac{2}{1-2x}+3x,$$

而
$$\frac{2}{1-2x}=2\sum_{n=0}^{\infty}2^n x^n=\sum_{n=0}^{\infty}2^{n+1}x^n,$$

所以有

$$a_n = \begin{cases} 2^{n+1}, & n \neq 1, \\ 2^2 + 3 = 7, & n = 1. \end{cases}$$

【例 8.22】 计算级数$\{n^2\}$的和

$$1^2 + 2^2 + \cdots + n^2.$$

解 先求$\{n^2\}$的生成函数$A(x) = \sum_{n=0}^{\infty} n^2 x^n$. 由

$$\frac{1}{(1-x)^2} = \sum_{n=1}^{\infty} n x^{n-1}$$

得

$$\frac{x}{(1-x)^2} = \sum_{n=1}^{\infty} n x^n.$$

对上式两边微商得

$$\frac{1+x}{(1-x)^3} = \sum_{n=1}^{\infty} n^2 x^{n-1},$$

所以有

$$A(x) = \sum_{n=0}^{\infty} n^2 x^n = \sum_{n=1}^{\infty} n^2 x^n = \frac{x(1+x)}{(1-x)^3}.$$

令$b_n = \sum_{i=1}^{n} i^2$,根据性质 6 可知$\{b_n\}$的生成函数是

$$B(x) = \frac{A(x)}{1-x} = \frac{x(1+x)}{(1-x)^4} = \frac{x}{(1-x)^4} + \frac{x^2}{(1-x)^4}.$$

$\frac{x}{(1-x)^4}$的展开式中x^n的系数是

$$\frac{(n+3)(n+2)(n+1)}{3!},$$

所以$B(x)$的展开式中x^n的系数是

$$b_n = \frac{(n+2)(n+1)n}{6} + \frac{(n+1)n(n-1)}{6} = \frac{n(n+1)(2n+1)}{6},$$

从而得到级数和

$$1^2 + 1^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

§8.4 生成函数与组合计数

生成函数在组合计数问题中有着广泛的应用. 用生成函数的方法可以求解递推方程,请看下面的例子.

【例 8.23】 求解递推方程

$$\begin{cases} a_n - 5a_{n-1} + 6a_{n-2} = 0, \\ a_0 = 1,\ a_1 = -2. \end{cases}$$

解 设 $A(x) = \sum_{n=0}^{\infty} a_n x^n$,则

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots,$$

$$-5x \cdot A(x) = -5a_0 x - 5a_1 x^2 - 5a_2 x^3 - \cdots,$$

$$6x^2 \cdot A(x) = 6a_0 x^2 + 6a_1 x^3 + \cdots.$$

把以上三个式子的两边分别相加得

$$(1 - 5x + 6x^2) \cdot A(x) = a_0 + (a_1 - 5a_0)x,$$

代入初值 $a_0 = 1, a_1 = -2$ 得

$$A(x) = \frac{1 - 7x}{1 - 5x + 6x^2}.$$

由部分分式的方法得

$$A(x) = \frac{5}{1 - 2x} - \frac{4}{1 - 3x} = 5\sum_{n=0}^{\infty} 2^n x^n - 4\sum_{n=0}^{\infty} 3^n x^n,$$

从而得到

$$a_n = 5 \cdot 2^n - 4 \cdot 3^n,\ n \geqslant 0.$$

【例 8.24】 求解递推方程

$$\begin{cases} h_n = \sum_{k=1}^{n-1} h_k h_{n-k}, & n \geqslant 2, \\ h_1 = 1. \end{cases}$$

解 这是一个非线性的递推方程，令

$$H(x)=\sum_{n=1}^{\infty}h_nx^n,$$

把上式两边平方得

$$H^2(x)=\Big(\sum_{k=1}^{\infty}h_kx^k\Big)\Big(\sum_{l=1}^{\infty}h_lx^l\Big)$$

$$=\sum_{n=2}^{\infty}x^n\sum_{k=1}^{n-1}h_kh_{n-k}=\sum_{n=2}^{\infty}h_nx^n=H(x)-h_1x,$$

代入初值 $h_1=1$ 得

$$H^2(x)=H(x)-x,$$

解这个关于 $H(x)$ 的一元二次方程得

$$H_1(x)=\frac{1+\sqrt{1-4x}}{2},\quad H_2(x)=\frac{1-\sqrt{1-4x}}{2}.$$

因为 $H(0)=0$，开方应该取负号，故舍去 $H_1(x)$，得

$$H(x)=\frac{1-\sqrt{1-4x}}{2}=\frac{1}{2}-\frac{1}{2}(1-4x)^{\frac{1}{2}}.$$

根据牛顿二项式定理得

$$(1-4x)^{\frac{1}{2}}=1+\sum_{n=1}^{\infty}\binom{\frac{1}{2}}{n}(-4x)^n \qquad |4x|<1$$

$$=1+\sum_{n=1}^{\infty}\frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)}{n!}2^{2n}\cdot(-1)^n\cdot x^n$$

$$=1+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}1\cdot 3\cdot 5\cdot\cdots\cdot(2n-3)}{2^n\cdot n!}(-1)^n\cdot 2^{2n}\cdot x^n$$

$$=1+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(2n-2)!}{2^n\cdot n!\cdot 2^{n-1}\cdot(n-1)!}(-1)^n2^{2n}x^n$$

$$=1+\sum_{n=1}^{\infty}\frac{1}{n}(-2)\binom{2n-2}{n-1}x^n,$$

因此有

$$H(x)=\frac{1}{2}-\frac{1}{2}\left[1+\sum_{n=1}^{\infty}\frac{1}{n}(-2)\binom{2n-2}{n-1}x^n\right]$$
$$=\sum_{n=1}^{\infty}\frac{1}{n}\binom{2n-2}{n-1}x^n,$$

从而得到原递推方程的解

$$h_n=\frac{1}{n}\binom{2n-2}{n-1}.$$

下面考察多重集的r-组合数. 设多重集$S=\{\infty\cdot a_1,\infty\cdot a_2,\cdots,\infty\cdot a_k\}$,$S$ 的 r-组合数恰为方程

$$x_1+x_2+\cdots+x_k=r$$

的非负整数解的个数. 设这个数为 a_r,且令数列$\{a_r\}$ 的生成函数为 $A(y)$.

做幂级数

$$(1+y+y^2+\cdots)^k, \tag{8.10}$$

把这个式子展开以后,它的各项都是如下形式:

$$y^{x_1}y^{x_2}\cdots y^{x_k}=y^{x_1+x_2+\cdots+x_k},$$

其中 y^{x_1} 来自第一个因式$(1+y+y^2+\cdots)$,y^{x_2} 来自第二个因式$(1+y+y^2+\cdots)$,$\cdots$,y^{x_k} 来自第 k 个因式$(1+y+y^2+\cdots)$,且 $x_1,x_2,\cdots,x_k$ 都是非负整数. 不难看出式 8.10 的展开式中 y^r 的系数对应了方程 $x_1+x_2+\cdots+x_k=r$ 的非负整数解的个数,所以 8.10 式就是$\{a_r\}$ 的生成函数 $A(y)$. 而

$$A(y)=\frac{1}{(1-y)^k}=\sum_{r=0}^{\infty}\binom{k+r-1}{r}y^r, \qquad \text{(见 8.9 式)},$$

所以有

$$a_r=\binom{k+r-1}{r}.$$

设多重集 $S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$，$S$ 的 r- 组合数 a_r 相当于方程

$$\begin{cases}x_1+x_2+\cdots+x_k=r,\\ x_i\leqslant n_i, \qquad i=1,2,\cdots,k\end{cases}$$

的非负整数解的个数. 设数列 $\{a_r\}$ 的生成函数为 $A(y)$，类似于前边的分析可以知道

$$A(y)=(1+y+y^2+\cdots+y^{n_1})(1+y+y^2+\cdots+y^{n_2})\cdot\cdots\cdot(1+y+y^2+\cdots+y^{n_k}).$$

而 $A(y)$ 的展式中 y^r 的系数 a_r 就是所求的多重集 S 的 r- 组合数.

【例 8.25】 求 $S=\{3\cdot a,4\cdot b,5\cdot c\}$ 的 10- 组合数.

解 设 S 的 r- 组合数为 a_r，则 $\{a_r\}$ 的生成函数为

$$\begin{aligned}A(y)&=(1+y+y^2+y^3)(1+y+y^2+y^3+y^4)\\&\quad(1+y+y^2+y^3+y^4+y^5)\\&=(1+2y+3y^2+4y^3+4y^4+3y^5+2y^6+y^7)\\&\quad(1+y+y^2+y^3+y^4+y^5).\end{aligned}$$

上式中 y^{10} 的系数为

$$3+2+1=6,$$

所以 $a_{10}=6$.

【例 8.26】 设多重集 $S=\{\infty\cdot a_1,\infty\cdot a_2,\cdots,\infty\cdot a_k\}$，求 S 的每个元素只出现偶数次的 r- 组合数 a_r.

解 设 $\{a_r\}$ 的生成函数为 $A(y)$，则

$$\begin{aligned}A(y)&=(1+y^2+y^4+\cdots)^k=\frac{1}{(1-y^2)^k}\\&=1+ky^2+\binom{k+1}{2}y^4+\cdots+\binom{k+n-1}{n}y^{2n}+\cdots,\end{aligned}$$

从而得到

$$a_r=\begin{cases}\dbinom{k+n-1}{n}, & r=2n,\\ 0, & r=2n+1,\end{cases}\qquad n=0,1,\cdots.$$

到此为止，我们已经给出了多重集的 r- 组合的计数方法. 与这个问题相关的另一个组合计数问题 —— 不定方程整数解的计数也可以使用生成函数的方法来求解.

【例 8.27】 求方程 $x_1+x_2+x_3=1$ 的整数解的个数，其中 $x_1, x_2, x_3>-5$.

解 做变换，令 $x_1=x'_1-4$，$x_2=x'_2-4$，$x_3=x'_3-4$，则原方程变成

$$\begin{cases} x'_1+x'_2+x'_3=13, \\ x'_1, x'_2, x'_3 \in N, \end{cases}$$

设该方程的解的个数为 a_{13}，则 $\{a_r\}$ 的生成函数是

$$A(y)=\frac{1}{(1-y)^3}=\sum_{r=0}^{\infty}\binom{r+2}{2}y^r,$$

所以有

$$a_{13}=\binom{13+2}{2}=105,$$

即原方程的整数解有 105 个.

【例 8.28】 求不定方程 $x_1+2x_2=15$ 的非负整数的解的个数.

解 设方程的非负整数解个数为 a_{15}，则 $\{a_r\}$ 的生成函数

$$\begin{aligned} A(y) &= (1+y+y^2+\cdots)(1+y^2+y^4+\cdots) \\ &= \frac{1}{1-y}\cdot\frac{1}{1-y^2} \\ &= \frac{1}{2(1-y)^2}+\frac{1}{4(1-y)}+\frac{1}{4(1+y)} \\ &= \frac{1}{2}\sum_{r=0}^{\infty}(r+1)y^r+\frac{1}{4}\sum_{r=0}^{\infty}y^r+\frac{1}{4}\sum_{r=0}^{\infty}(-1)^r y^r, \end{aligned}$$

因此有

$$a_r=\frac{1}{2}(r+1)+\frac{1}{4}+\frac{1}{4}(-1)^r.$$

$$a_{15} = \frac{1}{2} \times 16 + \frac{1}{4} - \frac{1}{4} = 8.$$

一般说来，令不定方程

$$p_1x_1 + p_2x_2 + \cdots + p_kx_k = r, \qquad (8.11)$$

$$p_1,\ p_2, \cdots, p_k \text{ 为正整数}$$

的非负整数解的个数为 a_r，考虑下面的函数

$$A(y) = [1 + y^{p_1} + (y^{p_1})^2 + \cdots] \cdot [1 + y^{p_2} + (y^{p_2})^2 + \cdots] \cdot \cdots \cdot [1 + y^{p_k} + (y^{p_k})^2 + \cdots],$$

$A(y)$ 的展开式的每一项都是如下形式：

$$y^{p_1x_1} \cdot y^{p_2x_2} \cdot \cdots \cdot y^{p_kx_k} = y^{p_1x_1+p_2x_2+\cdots+p_kx_k},$$

其中 $x_1, x_2, \cdots, x_k$ 为非负整数，所以 $A(y)$ 的展开式中 y^r 的系数就是方程

$$p_1x_1 + p_2x_2 + \cdots + p_kx_k = r$$

的非负整数解的个数. 把 $A(y)$ 变形为

$$A(y) = \frac{1}{(1 - y^{p_1})(1 - y^{p_2})\cdots(1 - y^{p_k})},$$

这就是 $\{a_r\}$ 的生成函数.

不难看出当 $p_1 = p_2 = \cdots = p_k = 1$ 时，$A(y) = \frac{1}{(1 - y)^k}$ 就是方程 $x_1 + x_2 + \cdots + x_k = r$ 的非负整数解的个数序列 $\{a_r\}$ 的生成函数.

如果在式 8.11 的不定方程中限制某个 x_i 的大小为 $m_i \leqslant x_i \leqslant n_i$，其中 m_i，n_i 为整数，则在生成函数 $A(y)$ 中相应于 x_i 的部分应改写为

$$(y^{p_im_i} + y^{p_i(m_i+1)} + \cdots + y^{p_in_i}).$$

这样就可以解决加了限制条件的不定方程的整数解问题.

最后我们考虑一个新的组合计数问题 —— 正整数的剖分问题.

所谓正整数的剖分，就是把正整数 N 表成若干个正整数之和.

剖分可以分成无序剖分和有序剖分，不允许重复的剖分和允许重复的剖分．按照上述的性质可将 4 的剖分列成表 8.1.

表 8.1

	有 序	无 序
不允许重复	$4=4, 4=1+3, 4=3+1$	$4=4, 4=1+3$
允许重复	$4=4, 4=1+3, 4=3+1$, $4=2+2, 4=2+1+1$, $4=1+2+1, 4=1+1+2$, $4=1+1+1+1$	$4=4, 4=1+3$, $4=2+2$, $4=1+1+2$, $4=1+1+1+1$

先考虑无序剖分的计数问题．

1. 将 N 无序剖分成正整数 $\alpha_1, \alpha_2, \cdots, \alpha_n$，且不允许重复．

这个问题对应于不定方程

$$\begin{cases} \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = N, \\ 0 \leqslant x_i \leqslant 1,\ i = 1, 2, \cdots, n \end{cases}$$

的整数解问题．令 a_N 表示 N 的剖分方案数，则 $\{a_N\}$ 的生成函数是

$$A(y) = (1 + y^{\alpha_1})(1 + y^{\alpha_2})\cdots(1 + y^{\alpha_n}). \tag{8.12}$$

特别地当 $\alpha_1 = 1, \alpha_2 = 2, \cdots, \alpha_n = n$ 时把这个生成函数记作 $A_n(y)$，

$$A_n(y) = (1 + y)(1 + y^2)\cdots(1 + y^n). \tag{8.13}$$

2. 将 N 无序剖分成正整数 $\alpha_1, \alpha_2, \cdots, \alpha_n$，且允许重复．

这个问题对应于不定方程

$$\begin{cases} \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = N, \\ 0 \leqslant x_i,\ i = 1, 2, \cdots, n \end{cases}$$

的整数解问题．令 a_N 表示 N 的剖分方案数，则 $\{a_N\}$ 的生成函数是

$$\begin{aligned} G(y) &= (1 + y^{\alpha_1} + y^{2\alpha_1} + \cdots)\cdot(1 + y^{\alpha_2} + y^{2\alpha_2} + \cdots)\cdots \\ &\quad (1 + y^{\alpha_n} + y^{2\alpha_n} + \cdots) \\ &= \frac{1}{(1 - y^{\alpha_1})(1 - y^{\alpha_2})\cdots(1 - y^{\alpha_n})}. \end{aligned} \tag{8.14}$$

特别地当 $\alpha_1 = 1, \alpha_2 = 2, \cdots, \alpha_n = n$ 时把这个生成函数记作 $G_n(y)$，

$$G_n(y) = \frac{1}{(1-y)(1-y^2)\cdots(1-y^n)}. \qquad (8.15)$$

【例 8.29】 对 N 进行无序的允许重复的任意剖分，设剖分方案数为 $P(N)$，求 $\{P(N)\}$ 的生成函数 $G(y)$.

解 这相当于把 N 无序剖分成 $1,2,\cdots,n,\cdots$，且允许重复的剖分方案数，类似于 8.15 式有

$$G(y) = \frac{1}{(1-y)(1-y^2)\cdots(1-y^n)}\cdots.$$

【例 8.30】 对 N 进行无序且允许重复的剖分，使得剖分后的正整数都是奇数，求这种剖分方案数 $\{P_0(N)\}$ 的生成函数 $G_0(y)$.

解 这是把 N 剖分成 $1,3,5,\cdots$，且允许重复的剖分. 类似 8.14 式得

$$G_0(y) = \frac{1}{(1-y)(1-y^3)\cdots(1-y^{2n+1})\cdots}.$$

【例 8.31】 对 N 进行无序剖分，使得剖分后的整数各不相等，求这种剖分方案数 $\{P_d(N)\}$ 的生成函数 $G_d(y)$.

解 这相当于把 N 剖分成 $1,2,\cdots,n,\cdots$，但不允许重复的剖分. 类似于式 8.13 有

$$G_d(y) = (1+y)(1+y^2)\cdots(1+y^n)\cdots.$$

【例 8.32】 对 N 进行无序剖分，使得剖分后的整数都是 2 的幂，求这种剖分的方法数 $\{P_t(N)\}$ 的生成函数 $G_t(y)$.

解 这相当于把 N 剖分成 $1,2,4,8,\cdots$，但不允许重复的剖分，类似于 8.12 式有

$$G_t(y) = (1+y)(1+y^2)(1+y^4)\cdots.$$

【例 8.33】 把 N 无序剖分成 $1,2,\cdots n$，允许重复且剖分后的整数中至少有一个 n 的剖分方案数为 $P_n(N)$，求 $\{P_n(N)\}$ 的生成函数 $G(y)$.

解 $G(y) = (1+y+y^2+\cdots)(1+y^2+y^4+\cdots)$

$$\cdot \cdots \cdot (1 + y^{n-1} + y^{2(n-1)} + \cdots)(y^n + y^{2n} + \cdots)$$

$$= \frac{y^n}{(1-y)(1-y^2)\cdots(1-y^n)}.$$

不难看出

$$G(y)=\frac{1}{(1-y)(1-y^2)\cdots(1-y^n)}-\frac{1-y^n}{(1-y)(1-y^2)\cdots(1-y^n)}$$

$$= G_n(y) - G_{n-1}(y),$$

其中$G_n(y)$对应于把N无序剖分成$1,2,\cdots,n$且允许重复的方案数，$G_{n-1}(y)$对应于把N无序剖分成$1,2,\cdots,n-1$且允许重复的方案数.

关于$P_0(N)$,$P_d(N)$,$P_t(N)$与$P(N)$有以下的定理.

定理 8.8　对一切N有$P_0(N) = P_d(N)$.

证　只须证明它们对应的生成函数相等就可以了.

$$G_d(y) = (1+y)(1+y^2)\cdots(1+y^n)\cdots$$

$$= \frac{1-y^2}{1-y}\cdot\frac{1-y^4}{1-y^2}\cdot\cdots\cdot\frac{1-y^{2n}}{1-y^n}\cdot\cdots$$

$$= \frac{1}{(1-y)(1-y^3)(1-y^5)\cdots}$$

$$= G_0(y).$$

▮

定理 8.9　对一切N有$P_t(N) = 1$.

证　$G_t(y) = (1+y)(1+y^2)(1+y^4)\cdots$

$$= \frac{1-y^2}{1-y}\cdot\frac{1-y^4}{1-y^2}\cdot\frac{1-y^8}{1-y^4}\cdot\cdots$$

$$= \frac{1}{1-y}$$

$$= 1 + y + y^2 + y^3 + \cdots,$$

从而有$P_t(N) = 1$.　▮

定理8.9说明任何一个十进制的正整数N可以唯一地表成一个二进制数，而这正是计算机能够工作的基础.

定理 8.10　对一切 N 有 $P(N) < e^{3\sqrt{N}}$.

证　由 $\{P(N)\}$ 的生成函数

$$G(y) = \frac{1}{(1-y)(1-y^2)(1-y^3)\cdots}$$

得

$$\ln G(y) = -\ln(1-y) - \ln(1-y^2) - \ln(1-y^3) - \cdots,$$

而

$$-\ln(1-y) = y + \frac{y^2}{2} + \frac{y^3}{3} + \cdots,$$

从而

$$\begin{aligned}\ln G(y) &= \left(y + \frac{y^2}{2} + \frac{y^3}{3} + \cdots\right) + \left(y^2 + \frac{y^4}{2} + \frac{y^6}{3} + \cdots\right) \\ &\quad + \left(y^3 + \frac{y^6}{2} + \frac{y^9}{3} + \cdots\right) + \cdots \\ &= (y + y^2 + y^3 + \cdots) + \frac{1}{2}(y^2 + y^4 + y^6 + \cdots) \\ &\quad + \frac{1}{3}(y^3 + y^6 + y^9 + \cdots) + \cdots \\ &= \frac{y}{1-y} + \frac{y^2}{2(1-y^2)} + \frac{y^3}{3(1-y^3)} + \cdots. \qquad ①\end{aligned}$$

先看 $\frac{y^n}{1-y^n}$，当 $0 < y < 1$ 时有

$$y^{n-1} < y^{n-2} < \cdots < y^2 < y < 1,$$

所以有

$$y^{n-1} < \frac{1 + y + y^2 + \cdots + y^{n-1}}{n},$$

即

$$\frac{y^{n-1}}{1 + y + y^2 + \cdots + y^{n-1}} < \frac{1}{n},$$

从而有

$$\frac{y^n}{1-y^n}=\frac{y}{1-y}\cdot\frac{y^{n-1}}{1+y+y^2+\cdots+y^{n-1}}<\frac{1}{n}\frac{y}{1-y}.$$

把以上结果代入式 ① 得

$$\ln G(y)<\frac{y}{1-y}+\left(\frac{1}{2}\right)^2\frac{y}{1-y}+\left(\frac{1}{3}\right)^2\frac{y}{1-y}+\cdots$$

$$=\frac{y}{1-y}\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\right).$$

由于

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots<1+\int_1^\infty\frac{1}{x^2}\mathrm{d}x=2,$$

$$\ln G(y)<\frac{2y}{1-y}.$$

又因为

$$P(N)y^N<G(y),$$

所以

$$\ln P(N)+N\ln y<\ln G(y)<\frac{2y}{1-y},$$

即

$$\ln P(N)<\frac{2y}{1-y}-N\ln y=\frac{2y}{1-y}+N(-\ln y).$$

当 $0<y<1$ 时有

$$-\ln y=\ln\frac{1}{y}<\frac{1}{y}-1=\frac{1-y}{y},$$

因此

$$\ln P(N)<\frac{2y}{1-y}+N\frac{1-y}{y}.$$

取 $y=\frac{\sqrt{N}}{\sqrt{N}+1}$,代入上式得

$$\ln P(N)<3\sqrt{N},$$

从而有

$$P(N) < e^{3\sqrt{N}}.$$ ∎

定理 8.11　当 $N \geqslant 2$ 时有

$$2^{[\sqrt{N}]} \leqslant P(N),$$

其中$[\sqrt{N}]$是小于等于$\sqrt{N}$的最大整数.

证　令 $S = \{1,2,\cdots,[\sqrt{N}]\}$. 任取 S 的一个 r 子集 $H(0 \leqslant r \leqslant [\sqrt{N}])$，都可以确定 N 的一个剖分. 若$H = \varnothing$，令 $N = N$. 若 $H \neq \varnothing$，设 $H = \{a_1,a_2,\cdots,a_r\}$，易见

$$a_1 + a_2 + \cdots + a_r \leqslant 1 + 2 + \cdots + [\sqrt{N}] \leqslant [\sqrt{N}]^2 \leqslant N,$$

因此

$$N = a_1 + a_2 + \cdots + a_r + (N - a_1 - a_2 - \cdots - a_r)$$

是 H 所确定的剖分，不难证明当 $N \geqslant 2$ 时，不同的子集 H 所确定的剖分也不相同. S 的不同子集个数为 $2^{[\sqrt{N}]}$，因此得到

$$2^{[\sqrt{N}]} \leqslant P(N),\ N \geqslant 2.$$ ∎

定理8.10和8.11分别给出当对N进行无序的允许重复的任意剖分时剖分方案数 $P(N)$ 的上界和下界.

关于无序剖分问题我们已经得到了许多的结果. 下面考虑一个新的无序剖分的问题. 如果要求把 N 正好无序剖分成 k 个正整数之和，$k \leqslant r$，且允许重复，那么剖分方案数是多少？我们采用组合对应的方法来求解.

定理 8.12　设 $P_1(N)$ 表示把 N 正好无序剖分成 $k(k \leqslant r)$ 个部分并且在剖分中允许重复的方案数，设 $P_r(N)$ 表示把 N 无序剖分成不大于 r 的正整数且允许重复的方案数，则有

$$P_1(N) = P_r(N).$$

证　设

$$N = \alpha_1 + \alpha_2 + \cdots + \alpha_k$$

是任意的无序剖分，且满足 $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_k$. 我们构造一个图，叫做

该剖分的Ferrers图. 对应于α_1,在图的第一列向上放α_1个圆点,对应于α_2,在图的第二列向上放α_2个圆点,…,对应于α_k,在图的第k列向上放α_k个圆点. 例如剖分

$$18 = 5 + 3 + 3 + 3 + 2 + 2$$

的 Ferrers 图如图 8.4 所示.

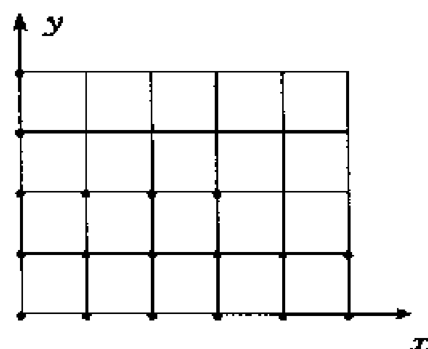


图 8.4

不难看出 Ferrers 图有以下特点:

1. 如果点(i, j)在图上,则$i \geqslant 0$, $j \geqslant 0$.

2. 如果点(i, j)在图上,则对于任意的非负整数i', j',满足$0 \leqslant i' \leqslant i$, $0 \leqslant j' \leqslant j$,有$(i', j')$点也在图上.

3. 把一个 Ferrers 图沿$y = x$直线翻转180°得到的是另一个剖分的Ferrers图,我们称这两个关于$y = x$直线成对称分布的Ferrers图是共轭的,相应的两个剖分也叫做**共轭的剖分**.

对于N的一个允许重复的无序剖分,如果剖分成恰好k个正整数之和$(k \leqslant r)$,则它的Ferrers图至多r列. 而它的共轭Ferrers图中每列至多r个点,即共轭剖分正好是把N无序剖分成不大于r的正整数且允许重复的一种方案. 反之也同样成立. 所以$P_1(N) = P_r(N)$.

∎

前边已经对$P_r(N)$的生成函数作了介绍,有了$P_r(N)$,根据这个定理也就得到了$P_1(N)$.

【例 8.34】 求把 6 无序剖分成$k(k \leqslant 3)$个部分且允许重复的方案数.

解 考虑将6无序剖分成不大于3的正整数且允许重复的方案数$P_3(6)$. 相应的生成函数是

$$\begin{aligned}G(y) &= (1 + y + y^2 + \cdots)(1 + y^2 + y^4 + \cdots)\\&\quad(1 + y^3 + y^6 + \cdots)\\&= (1 + y + 2y^2 + 2y^3 + 3y^4 + 3y^5 + 4y^6 + \cdots)\\&\quad(1 + y^3 + y^6 + \cdots)\end{aligned}$$

$$=1+y+2y^2+3y^3+4y^4+5y^5+7y^6+\cdots.$$

展开式中 y^6 的系数是7,即 $P_3(6)=7$. 由定理8.12,把6无序剖分成至多3个部分的允许重复的方案数是7. 列出这7种方案如下:

$6=6$, $6=5+1$, $6=4+2$, $6=3+3$,

$6=2+2+2$, $6=4+1+1$, $6=3+2+1$.

关于无序剖分的问题就讨论到这里. 下面的定理是关于有序剖分问题的.

定理 8.13 把 N 有序剖分成 r 个部分且允许重复的方案数是 $\binom{N-1}{r-1}$.

证 设 N 的有序剖分是

$$N=\alpha_1+\alpha_2+\cdots+\alpha_r.$$

建立序列 $S_1,S_2,\cdots,S_r$,使得

$$S_1=\alpha_1,$$
$$S_2=\alpha_1+\alpha_2,$$
$$\cdots$$
$$S_r=\alpha_1+\alpha_2+\cdots+\alpha_r=N.$$

易见 $0<S_1<S_2<\cdots<S_r=N$,且对任意的 $i=1,2,\cdots,r-1$ 有 $S_i\in\{1,2,\cdots,N-1\}$. 反之,任意给定一个序列 $S_1,S_2,\cdots,S_{r-1}$,满足 $0<S_1<S_2<\cdots<S_{r-1}<N$,就可以唯一地确定正整数 $\alpha_1,\alpha_2,\cdots,\alpha_r$,从而得到 N 的一个有序剖分. 所以把 N 有序剖分成 r 个部分的方案数等于从集合 $\{1,2,\cdots,N-1\}$ 中选取 $r-1$ 个数 $S_1,S_2,\cdots,S_{r-1}$ 的方法数,即 $\binom{N-1}{r-1}$. ∎

推论 把 N 进行任意的允许重复的有序剖分的方案数是

$$\sum_{r=1}^{N}\binom{N-1}{r-1}=2^{N-1}.$$

证 将 N 的有序剖分按剖分成的部分数 r 进行分类,$r=1,2,$

$\cdots,N$. 根据加法法则和定理 8.13，剖分方案数是 $\sum_{r=1}^{N}\binom{N-1}{r-1}$，而由二项式定理的推论(7.4 式)得 $\sum_{r=1}^{N}\binom{N-1}{r-1}=2^{N-1}$. ∎

最后我们讨论关于 N 的不允许重复的有序剖分问题. 根据前面的分析. 我们已经得到了关于 N 的不允许重复的无序剖分问题的生成函数(例 8.31). 针对每一种无序剖分的方案，将各个剖成的部分进行排列，就得到所有的有序剖分的方案了，显然这种剖分也是不允许重复的剖分.

§8.5 指数生成函数与多重集的排列问题

定义 8.7 设 $a_0,a_1,\cdots,a_n$ 是一个数列，它的**指数生成函数**记作 $A_e(x)$，且

$$A_e(x)=\sum_{n=0}^{\infty}a_n\frac{x^n}{n!}.$$

【例 8.35】 求以下数列 $\{a_n\},\{b_n\},\{c_n\}$ 的指数生成函数 $A_e(x)$，$B_e(x)$ 和 $C_e(x)$.

(1) $a_n=P(m,n)$，m 为给定正整数；

(2) $b_n=1$；

(3) $c_n=t^n$，t 为给定常数.

解 (1) $A_e(x)=\sum_{n=0}^{\infty}P(m,n)\frac{x^n}{n!}=\sum_{n=0}^{\infty}C(m,n)x^n=(1+x)^m$；

(2) $B_e(x)=\sum_{n=0}^{\infty}1\cdot\frac{x^n}{n!}=\mathrm{e}^x$；

(3) $C_e(x)=\sum_{n=0}^{\infty}t^n\frac{x^n}{n!}=\sum_{n=0}^{\infty}\frac{(tx)^n}{n!}=\mathrm{e}^{tx}$.

下面考虑指数生成函数的性质.

定理 8.14 设数列 $\{a_n\},\{b_n\}$ 的指数生成函数分别为 $A_e(x)$ 和 $B_e(x)$，则

$$A_e(x)\cdot B_e(x)=\sum_{n=0}^{\infty}c_n\frac{x^n}{n!},$$

其中

$$c_n=\sum_{k=0}^{\infty}\binom{n}{k}a_kb_{n-k}.$$

证

$$\sum_{n=0}^{\infty}c_n\frac{x^n}{n!}=A_e(x)\cdot B_e(x)$$

$$=\sum_{k=0}^{\infty}a_k\frac{x^k}{k!}\cdot\sum_{l=0}^{\infty}b_l\frac{x^l}{l!}.$$

比较上式两边 x^n 的系数得

$$\frac{c_n}{n!}=\sum_{k=0}^{n}\frac{a_k}{k!}\cdot\frac{b_{n-k}}{(n-k)!}=\frac{1}{n!}\sum_{k=0}^{n}\frac{n!}{k!(n-k)!}a_kb_{n-k}$$

$$=\frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}a_kb_{n-k},$$

从而有

$$c_n=\sum_{k=0}^{n}\binom{n}{k}a_kb_{n-k}.$$

∎

【例 8.36】 设 $\{a_n\}$ 是一个数列，如果

$$b_n=\sum_{k=0}^{n}(-1)^k\binom{n}{k}a_k,$$

则

$$a_n=\sum_{k=0}^{n}(-1)^k\binom{n}{k}b_k.$$

证 设 $\{(-1)^na_n\}$ 的指数生成函数为 $A_e(x)$，则

$$A_e(x)=\sum_{n=0}^{\infty}(-1)^na_n\frac{x^n}{n!}.$$

上式两边同时乘以 e^x 得

$$e^x\cdot A_e(x)=e^x\left(\sum_{n=0}^{\infty}(-1)^na_n\frac{x^n}{n!}\right)$$

$$= \left(\sum_{n=0}^{\infty} \frac{x^n}{n!} \right) \left(\sum_{n=0}^{\infty} (-1)^n a_n \frac{x^n}{n!} \right)$$

$$= \sum_{n=0}^{\infty} \frac{x^n}{n!} \left(\sum_{k=0}^{n} (-1)^k \binom{n}{k} a_k \right) \quad \text{（根据定理 8.14）}$$

$$= \sum_{n=0}^{\infty} b_n \frac{x^n}{n!} = B_e(x).$$

所以有

$$\sum_{n=0}^{\infty} (-1)^n a_n \frac{x^n}{n!} = A_e(x)$$

$$= e^{-x} \cdot B_e(x)$$

$$= \left(\sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} \right) \left(\sum_{n=0}^{\infty} b_n \frac{x^n}{n!} \right)$$

$$= \sum_{n=0}^{\infty} \frac{x^n}{n!} \left(\sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} b_k \right).$$

比较上式两边 x^n 的系数得

$$(-1)^n a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k$$

$$= (-1)^n \sum_{k=0}^{n} (-1)^{-k} \binom{n}{k} b_k,$$

从而有

$$a_n = \sum_{k=0}^{n} (-1)^{-k} \binom{n}{k} b_k = \sum_{k=0}^{n} (-1)^k \binom{n}{k} b_k. \qquad \blacksquare$$

我们可以把 a_n 与 b_n 之间互逆的两个公式看作是一种组合变换. 可以通过组合变换的方法来证明组合恒等式.

【例 8.37】 证明

$$\sum_{k=1}^{n} (-1)^k \binom{n}{k} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} \right) = -\frac{1}{n}.$$

证 令 $a_0 = 0$, $a_k = -\frac{1}{k}$, $k = 1, 2, \cdots$,

$$b_0=0,\ b_n=\sum_{k=1}^{n}(-1)^k\binom{n}{k}a_k,\ n\geqslant 1,$$

则有

$$\begin{aligned} b_n &= \sum_{k=1}^{n}(-1)^k\binom{n}{k}a_k \qquad (n\geqslant 1)\\ &= \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}\frac{1}{k}\\ &= 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \quad \text{（参考习题七，30(4)）}. \end{aligned}$$

根据例 8.36 有

$$\begin{aligned} a_n &= \sum_{k=1}^{n}(-1)^k\binom{n}{k}b_k\\ &= \sum_{k=1}^{n}(-1)^k\binom{n}{k}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k}\right), \end{aligned}$$

而 $a_n=-\frac{1}{n}$，从而得到

$$\sum_{k=1}^{n}(-1)^k\binom{n}{k}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k}\right)=-\frac{1}{n}. \qquad \blacksquare$$

利用生成函数已经解决了多重集 $S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$ 的 r- 组合问题. 而利用指数生成函数可以解决多重集的 r- 排列问题.

定理 8.15 设多重集 $S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$. 对任意的非负整数 r，令 a_r 为 S 的 r- 排列数，设数列 $\{a_r\}$ 的指数生成函数为 $A_e(x)$，则

$$A_e(x)=f_{n_1}\cdot f_{n_2}\cdot\cdots\cdot f_{n_k}(x),$$

其中

$$f_{n_i}(x)=1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_i}}{n_i!},\ i=1,2,\cdots,k.$$

证 考察 $A_e(x)$ 的展开式中 x^r 的项，它一定是下面这种项之和：

$$\frac{x^{m_1}}{m_1!}\cdot\frac{x^{m_2}}{m_2!}\cdot\cdots\cdot\frac{x^{m_k}}{m_k!},$$

其中

$$m_1+m_2+\cdots+m_k=r,$$
$$0\leqslant m_i\leqslant n_i,\ i=1,2,\cdots,k.$$

而这种项又可以写作

$$\frac{x^{m_1+m_2+\cdots+m_k}}{m_1!m_2!\cdots m_k!}=\frac{r!}{m_1!m_2!\cdots m_k!}\frac{x^r}{r!}.$$

所以在 $A_e(x)$ 的展式中$\frac{x^r}{r!}$ 的系数是

$$a_r=\sum\frac{r!}{m_1!m_2!\cdots m_k!},$$

其中求和是对方程

$$\begin{cases}m_1+m_2+\cdots+m_k=r,\\ m_i\leqslant n_i,\ i=1,2,\cdots,k\end{cases}\qquad ①$$

的一切非负整数解来求. 另一方面，

$$\frac{r!}{m_1!m_2!\cdots m_k!}$$

就是 S 的 r 元子集$\{m_1\cdot a_1,m_2\cdot a_2,\cdots,m_k\cdot a_k\}$ 的全排列数. 如果对所有满足 ① 式的 $m_1,m_2,\cdots,m_k$ 求和，就是 S 的所有 r 元子集的排列数，即 S 的 r- 排列数. 所以 $A_e(x)$ 的展开式中$\frac{x^r}{r!}$ 的系数 a_r 就是多重集 S 的 r- 排列数. ∎

考虑多重集$S=\{\infty\cdot a_1,\infty\cdot a_2,\cdots,\infty\cdot a_k\}$，由这个定理可以知道当 n_i 是 ∞ 的时候，$i=1,2,\cdots,k$，有

$$f_{n_i}(x)=1+x+\frac{x^2}{2!}+\cdots=e^x,$$

从而得到

$$A_e(x) = (e^x)^k = e^{kx}$$
$$= 1 + kx + \frac{k^2}{2!}x^2 + \cdots + k^r\frac{x^r}{r!} + \cdots.$$

因此 S 的 r- 排列数是 k^r，与定理 7.4 的结果一致.

【例 8.38】 求 $S = \{2 \cdot a, 3 \cdot b\}$ 的 4- 排列数.

解 设 S 的 4- 排列数为 a_4，则 $\{a_n\}$ 的指数生成函数是

$$A_e(x) = \left(1 + x + \frac{x^2}{2!}\right)\left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!}\right)$$
$$= 1 + 2x + 4 \cdot \frac{x^2}{2!} + 7 \cdot \frac{x^3}{3!} + 10 \cdot \frac{x^4}{4!} + 10 \cdot \frac{x^5}{5!},$$

因此有 $a_4 = 10$. 列出这 10 个4-排列如下：

$$aabb,\ abab,\ abba,\ baab,\ baba,$$
$$bbaa,\ abbb,\ babb,\ bbab,\ bbba.$$

【例 8.39】 设多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$，若要求在 S 的 n- 排列中每种元素至少出现一次，求 S 的这种 n- 排列数.

解 设所求的 n- 排列数为 a_n，则 $\{a_n\}$ 的指数生成函数是

$$A_e(x) = \left(x + \frac{x^2}{2!} + \cdots\right)^k = (e^x - 1)^k,$$

所以

$$a_n = \sum \frac{n!}{m_1!m_2!\cdots m_k!},$$

其中求和是对方程 $m_1 + m_2 + \cdots + m_k = n$ 的一切正整数解来求.

【例 8.40】 用红、白、蓝三色涂色 $1 \times n$ 的方格，每个方格只能涂一种颜色，如果要求偶数个方格要涂成白色，问有多少种涂色方案?

解 设 a_n 表示涂色方案数，定义 $a_0 = 1$，又设多重集 $S = \{\infty \cdot R, \infty \cdot W, \infty \cdot B\}$，其中 R 代表红色，W 代表白色，B 代表蓝色，则涂色方案数 a_n 就是 S 的含有偶数个 W 的 n- 排列数. $\{a_n\}$ 的指

数生成函数为

$$A_e(x)=\left(1+\frac{x^2}{2!}+\frac{x^4}{4!}+\cdots\right)\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)^2$$

$$=\frac{1}{2}(e^x+e^{-x})\cdot e^{2x}=\frac{1}{2}(e^{3x}+e^x)$$

$$=\frac{1}{2}\sum_{n=0}^{\infty}3^n\frac{x^n}{n!}+\frac{1}{2}\sum_{n=0}^{\infty}\frac{x^n}{n!}=\sum_{n=0}^{\infty}\frac{3^n+1}{2}\frac{x^n}{n!},$$

所以

$$a_n=\frac{3^n+1}{2}.$$

这个问题也可以用递推方程的方法求解，根据题意列出递推方程如下：

$$\begin{cases}a_n=2a_{n-1}+3^{n-1}-a_{n-1},\\a_0=1.\end{cases}$$

即

$$\begin{cases}a_n-a_{n-1}=3^{n-1},\\a_0=1.\end{cases}$$

该方程的特解设为 $P\cdot 3^{n-1}$，代入解得 $P=\frac{3}{2}$，从而得到该方程的通解是

$$c\cdot 1^n+\frac{3^n}{2},$$

代入初值得 $c=\frac{1}{2}$，因此有 $a_n=\frac{3^n+1}{2}$.

§8.6 Catalan 数与 Stirling 数

给定一个平面点集 K，如果对 K 中任意两点 p 和 q，连接 p 和 q 的线段上的所有的点都在 K 中，则称点集是凸的.

设 R 是一个 n 条边的凸多边形区域，用 $n-3$ 条不在内部相交的对角线把 R 分成 $n-2$ 个三角形. 求有多少种不同的分法？

令 h_n 表示分一个 $n+1$ 条边的凸多边形为三角形的方法数. 定义 $h_1=1$. 当 $n=2$ 时, $n+1$ 边形就是三角形,所以 $h_2=1$. 当 $n\geqslant 3$ 时,考虑一个有 $n+1\geqslant 4$ 条边的凸多边形区域 R. 如图 8.5 所示,任取多边形的一条边 a, a 的两个端点记作 A_1, A_{n+1}. 以 a 为一条边,以多边形的任一端点 $A_{k+1}(k=1,2,\cdots,n-1)$ 与 A_1, A_{n+1} 的连线为两条边构成三角形 T. T 把 R 分割成 R_1 和 R_2 两部分. R_1 为 $k+1$ 边形, R_2 为 $n-k+1$ 边形,因此 R_1 可以用 h_k 种方法来划分, R_2 可以用 h_{n-k} 种方法来划分. 这就得到下面的递推方程

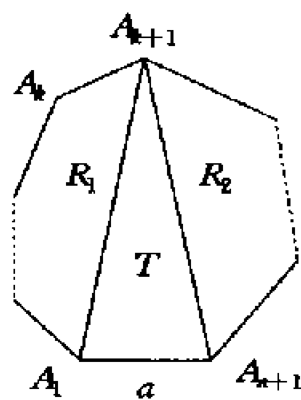


图 8.5

$$\begin{cases} h_n = \sum_{k=1}^{n-1} h_k h_{n-k}, & n\geqslant 2, \\ h_1 = 1. \end{cases} \tag{8.16}$$

根据例 8.24,该方程的解是

$$h_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

我们称 h_n 为 **Catalan 数**.

Catalan 数在组合计数问题中经常出现,下面给出一些例子.

在第七章我们讨论了从(0,0) 点到(n,n) 点的非降路径问题,其中从(0,0) 点到(n,n) 点除端点外不接触对角线的非降路径数是 $\frac{2}{n}\binom{2n-2}{n-1}$,而对角线一侧的非降路径数恰好是$\frac{1}{n}\binom{2n-2}{n-1}$,是第 n 个 Catalan 数 h_n. 类似地,不穿过对角线的从(0,0) 点到(n,n) 点的非降路径数是 $\frac{2}{n+1}\binom{2n}{n}$, 其中在对角线一侧的路径数是 $\frac{1}{n+1}\binom{2n}{n}$,这是第 $n+1$ 个 Catalan 数 h_{n+1}.

n 个数相乘,不改变它们的位置,只用括号表示不同的相乘顺

序，问可以构成多少个不同的乘积？

令 G_n 表示所求的乘积个数，那么有

$$\begin{cases} G_n = \sum_{k=1}^{n-1} G_k G_{n-k}, & n \geqslant 2, \\ G_1 = 1. \end{cases}$$

这个递推方程与 8.16 式完全一样，所以

$$G_n = \frac{1}{n}\binom{2n-2}{n-1}$$

是第 n 个 Catalan 数. 当 $n = 4$ 时，$G_4 = \frac{1}{4}\binom{6}{3} = 5$，这 5 种乘积列出来就是：

$$(((a_1a_2)a_3)a_4),\ ((a_1(a_2a_3))a_4),\ ((a_1a_2)(a_3a_4)),$$
$$(a_1(a_2(a_3a_4))),\ (a_1((a_2a_3)a_4)).$$

下面考虑 Stirling 数.

设有多项式

$$x(x-1)(x-2)\cdots(x-n+1),$$

它的展开式形如

$$s_n x^n - s_{n-1}x^{n-1} + s_{n-2}x^{n-2} - \cdots.$$

不考虑各项系数的符号，将 x^r 的系数的绝对值 s_r 记作 $\begin{bmatrix} n \\ r \end{bmatrix}$，则上面的展开式可写作

$$\begin{bmatrix} n \\ n \end{bmatrix}x^n - \begin{bmatrix} n \\ n-1 \end{bmatrix}x^{n-1} + \begin{bmatrix} n \\ n-2 \end{bmatrix}x^{n-2} - \cdots \pm \begin{bmatrix} n \\ 0 \end{bmatrix}.$$

称 $\begin{bmatrix} n \\ n \end{bmatrix}, \begin{bmatrix} n \\ n-1 \end{bmatrix}, \cdots, \begin{bmatrix} n \\ 0 \end{bmatrix}$ 这些数为**第一类 Stirling 数**。

第一类 Stirling 数具有下面的性质.

1. $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$, $\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!$, $\begin{bmatrix} n \\ n \end{bmatrix} = 1$, $\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2}$.

证 $\begin{bmatrix} n \\ 0 \end{bmatrix}$ 为 x^0 的系数，即多项式中的常数项，显然为 0.

$\begin{bmatrix}n\\1\end{bmatrix}$为 x 项的系数，$(x-1),(x-2),(x-n+1)$ 各因式在相乘时分别贡献负数 $-1,-2,\cdots,-(n-1)$，从而得到 x 项. 不考虑这些数的符号，它们的积是 $(n-1)!$，所以 $\begin{bmatrix}n\\1\end{bmatrix}=(n-1)!$.

$\begin{bmatrix}n\\n\end{bmatrix}$是 x^n 的系数，显然为 1.

$\begin{bmatrix}n\\n-1\end{bmatrix}$是 x^{n-1} 的系数，为了得到 x^{n-1}，n 个因式中只能有一个因式贡献常数，由加法法则这些常数的总和为

$$(-1)+(-2)+\cdots+[-(n-1)]=-\frac{n(n-1)}{2},$$

因此

$$\begin{bmatrix}n\\n-1\end{bmatrix}=\frac{n(n-1)}{2}=\binom{n}{2}.$$ ∎

2. 第一类 Stirling 数满足下面的递推方程：

$$\begin{bmatrix}n\\r\end{bmatrix}=(n-1)\begin{bmatrix}n-1\\r\end{bmatrix}+\begin{bmatrix}n-1\\r-1\end{bmatrix},\qquad n>r\geqslant 1. \tag{8.17}$$

证 考虑多项式

$$x(x-1)\cdots(x-n+2)$$
$$=\begin{bmatrix}n-1\\n-1\end{bmatrix}x^{n-1}-\begin{bmatrix}n-1\\n-2\end{bmatrix}x^{n-2}+\cdots\pm\begin{bmatrix}n-1\\0\end{bmatrix}x^0,$$

上式两边同乘以 $(x-n+1)$ 得

$$x(x-1)\cdots(x-n+1)$$
$$=\left(\begin{bmatrix}n-1\\n-1\end{bmatrix}x^{n-1}-\begin{bmatrix}n-1\\n-2\end{bmatrix}x^{n-2}+\cdots\pm\begin{bmatrix}n-1\\0\end{bmatrix}x^0\right)(x-n+1),$$

即

$$\begin{bmatrix}n\\n\end{bmatrix}x^n-\begin{bmatrix}n\\n-1\end{bmatrix}x^{n-1}+\cdots\pm\begin{bmatrix}n\\0\end{bmatrix}x^0$$

$$=\begin{bmatrix}n-1\\n-1\end{bmatrix}x^n-\begin{bmatrix}n-1\\n-2\end{bmatrix}x^{n-1}+\cdots\pm\begin{bmatrix}n-1\\0\end{bmatrix}x$$

$$-(n-1)\begin{bmatrix}n-1\\n-1\end{bmatrix}x^{n-1}+(n-1)\begin{bmatrix}n-1\\n-2\end{bmatrix}x^{n-2}\cdots$$

$$\mp(n-1)\begin{bmatrix}n-1\\0\end{bmatrix}x^0.$$

比较上式两边 x^r 的系数得

$$\begin{bmatrix}n\\r\end{bmatrix}=(n-1)\begin{bmatrix}n-1\\r\end{bmatrix}+\begin{bmatrix}n-1\\r-1\end{bmatrix}.$$ ▮

8.17 式与第七章学过的 Pascal 公式非常相似，仿照杨辉三角形，我们也可以构造关于第一类 Stirling 数的三角形. 请看图 8.6.

例如

$$\begin{bmatrix}5\\3\end{bmatrix}=(5-1)\begin{bmatrix}4\\3\end{bmatrix}+\begin{bmatrix}4\\2\end{bmatrix}$$

在图中就是

$$35=4\times6+11.$$

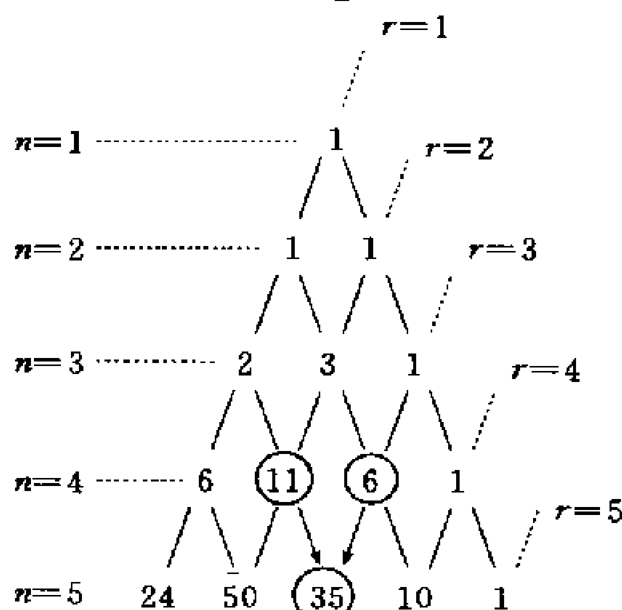


图 8.6

3. 第一类 Stirling 数对应的组合问题.

设 S_n 是 n 元对称群，则 S_n 中含有 r 个不相交轮换的置换恰为 $\begin{bmatrix}n\\r\end{bmatrix}$ 个. 证明如下：

假设 S_n 中含有 r 个不相交轮换的置换是 $\langle{n \atop r}\rangle$ 个. 这种置换可以从 S_{n-1} 中的含有 $r-1$ 个或者 r 个不相交轮换的置换通过加入文字 n 来构成. 如果 S_{n-1} 中的置换含有 $r-1$ 轮换，那么加入 (n) 后就得到 S_n 中恰含 r 个不相交轮换的置换. 如果 S_{n-1} 中的置换含有 r 个不相交

的轮换，那么必须将 n 加入其中的某个轮换之中，加入的方法为 $n-1$ 种. 从而得到以下的递推方程：

$$\begin{cases} \left\langle {n \atop r} \right\rangle = \left\langle {n-1 \atop r-1} \right\rangle + (n-1)\left\langle {n-1 \atop r} \right\rangle, \\ \left\langle {n \atop 0} \right\rangle = 0,\ \left\langle {n \atop 1} \right\rangle = (n-1)!. \end{cases}$$

这就是第一类 Stirling 数的递推方程. 所以有

$$\left\langle {n \atop r} \right\rangle = \begin{bmatrix} n \\ r \end{bmatrix}.$$

根据以上分析不难得到一个关于第一类 Stirling 数的恒等式

$$\sum_{r=1}^{n} \begin{bmatrix} n \\ r \end{bmatrix} = n!,$$

因为等式左边和右边都是 S_n 中的置换总数.

下面考虑第二类 Stirling 数，先给出有关的定义.

把 n 个不同的球放到 r 个相同的盒子里，假设没有空盒，则放球方案数记作 $\left\{ {n \atop r} \right\}$，称为**第二类 Stirling 数.**

例如 a,b,c,d 四个球，放到两个盒子里，不允许有空盒，则放球的方案有以下 7 种：

$a|bcd$, $b|acd$, $c|abd$, $d|abc$, $ab|cd$, $ac|bd$, $ad|bc$.

所以 $\left\{ {4 \atop 2} \right\} = 7$.

第二类 Stirling 数具有下面的性质.

1. $\left\{ {n \atop 0} \right\} = 0$, $\left\{ {n \atop 1} \right\} = 1$, $\left\{ {n \atop 2} \right\} = 2^{n-1} - 1$,

$\left\{ {n \atop n-1} \right\} = \binom{n}{2}$, $\left\{ {n \atop n} \right\} = 1$.

证 没有盒子，当然谈不到放法，所以 $\left\{ {n \atop 0} \right\} = 0$.

把 n 个不同的球放到一个盒子里只有一种放法，所以 $\left\{ {n \atop 1} \right\} = 1$.

把 n 个不同的球恰好放入两个相同的盒子里，我们先任意放一个球，比如说是 a_n，把它放到一个盒子里. 对于剩下的 $n-1$ 个球，每个球可以有两种选择：与 a_n 同在一个盒子里或不与 a_n 同在一个盒子里，由乘法法则有 2^{n-1} 种放法. 但其中有一种放法，就是 $n-1$ 个球都与 a_n 同放在一个盒子里的放法不符合要求，所以 $\left\{{n \atop 2}\right\} = 2^{n-1} - 1$.

要把 n 个不同的球正好放到 $n-1$ 个相同的盒子里，那么必须有一个盒子放两个球. 这两个球要从 n 个球中选取，有 $\binom{n}{2}$ 种选法，所以 $\left\{{n \atop n-1}\right\} = \binom{n}{2}$.

n 个不同的球放到 n 个相同的盒子里，不允许空盒，只有一种放法，就是每个盒子一个球，所以有 $\left\{{n \atop n}\right\} = 1$. ∎

2. 第二类 Stirling 数满足下面的递推方程：

$$\left\{{n \atop r}\right\} = r\left\{{n-1 \atop r}\right\} + \left\{{n-1 \atop r-1}\right\}, \qquad n > r \geqslant 1. \quad (8.18)$$

证 要把 n 个不同的球恰好放入 r 个盒子，先取一个球，比如说是 a_n，然后把所有的放法分成两类：

a_n 单独放在一个盒子里，放法为 $\left\{{n-1 \atop r-1}\right\}$ 种.

a_n 不是单独放在一个盒子里，可以先把其余的 $n-1$ 个球放到 r 个盒子里，有 $\left\{{n-1 \atop r}\right\}$ 种放法. 对于其中的任何一种放法，加入 a_n 的方法有 r 种，由乘法法则，放球的方法数是 $r\left\{{n-1 \atop r}\right\}$.

根据加法法则，等式成立. ∎

把这个性质与第一类 Stirling 数的性质 2 对比，也可以构造出关于第二类 Stirling 数的三角形. 请看图 8.7.

例如

$$\begin{Bmatrix}5\\3\end{Bmatrix}=3\begin{Bmatrix}4\\3\end{Bmatrix}+\begin{Bmatrix}4\\2\end{Bmatrix}.$$

在图上就是

$$25=3\times 6+7.$$

3. 关于放球问题的某些结果.

(1) n 个不同的球放到 m 个相同的盒子里,允许空盒,则放球方法数是

$$\begin{Bmatrix}n\\1\end{Bmatrix}+\begin{Bmatrix}n\\2\end{Bmatrix}+\cdots+\begin{Bmatrix}n\\m\end{Bmatrix}.$$

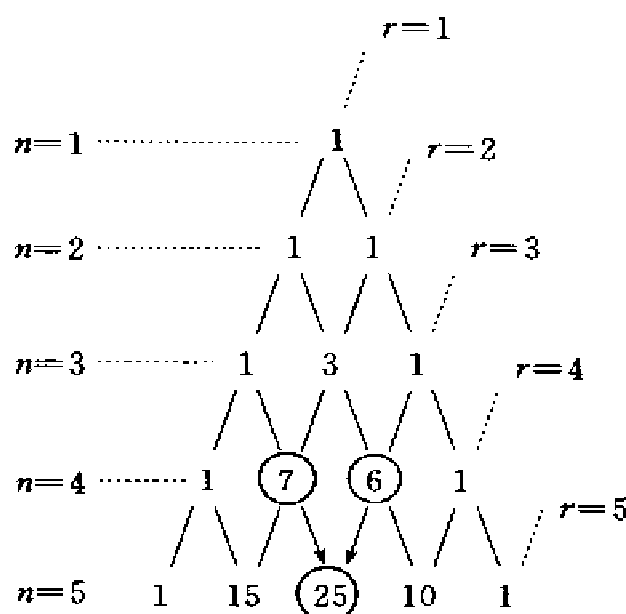


图 8.7

证 对任何正整数 k, $1\leqslant k\leqslant m$, $\begin{Bmatrix}n\\k\end{Bmatrix}$计数了 n 个不同的球恰好放入 k 个相同的盒子的放法,对 k 求和以后就得到 n 个不同的球放到 m 个相同的盒子且允许空盒的放法数. ∎

(2) n 个不同的球恰好放到 m 个不同的盒子里,则放球方法数是

$$m!\begin{Bmatrix}n\\m\end{Bmatrix}.$$

证 如果盒子不编号,那么 n 个不同的球正好放到 m 个盒子里的方法数是$\begin{Bmatrix}n\\m\end{Bmatrix}$. 对于其中的每一种放法,盒子有 $m!$ 种编号的方法. 由乘法法则,所求的放法数是 $m!\begin{Bmatrix}n\\m\end{Bmatrix}$. ∎

下面从另一个角度来考虑这个问题. 将 n 个不同的球放入 m 个不同的盒子,使得第一个盒子含有 n_1 个球,第二个盒子含有 n_2 个球,…,第 m 个盒子含有 n_m 个球,其中 $n_1,n_2,\cdots,n_m$ 是正整数,则这样的放法有$\binom{n}{n_1\ n_2\cdots n_m}$种. 如果对所有满足方程 $n_1+n_2+\cdots+n_m=n$

的一切正整数解 $n_1, n_2, \cdots, n_m$ 求和，即 $\sum\binom{n}{n_1\ n_2\cdots n_m}$，则计数了 n 个不同的球恰好放入 m 个不同的盒子的放法. 从而得到下面的等式

$$\sum\binom{n}{n_1\ n_2\cdots n_m} = m!\left\{{n \atop m}\right\},$$

其中求和是对方程 $n_1 + n_2 + \cdots + n_m = n$ 的一切正整数解来求.

(3) n 个不同的球放到 m 个不同的盒子里，允许空盒，则放球的方法数是

$$\binom{m}{1}\left\{{n \atop 1}\right\}\cdot 1! + \binom{m}{2}\left\{{n \atop 2}\right\}\cdot 2! + \cdots + \binom{m}{m}\left\{{n \atop m}\right\}\cdot m!.$$

证 对于任意的正整数 k，$1 \leqslant k \leqslant m$，$\binom{m}{k}$ 表示从 m 个盒子中选出 k 个盒子的方法数，而 $\left\{{n \atop k}\right\}\cdot k!$ 则表示把 n 个不同的球放到这 k 个不同的盒子的放法数. 根据乘法法则，$\binom{m}{k}\left\{{n \atop k}\right\}\cdot k!$ 就是把 n 个不同的球恰好放入 m 个不同的盒子里的 k 个盒子的放法数. 当对 k 求和后就得到 n 个不同的球放到 m 个不同的盒子且允许空盒的放法数. ∎

如果从另一个角度来考虑这个组合计数问题. n 个球中的每个球都有 m 种选择，由乘法法则，n 个不同的球放到 m 个不同的盒子且允许空盒的放法为 m^n 种，从而得到下面的等式.

$$m^n = \binom{m}{1}\left\{{n \atop 1}\right\}\cdot 1! + \binom{m}{2}\left\{{n \atop 2}\right\}\cdot 2! + \cdots + \binom{m}{m}\left\{{n \atop m}\right\}\cdot m!.$$

表 8.2 给出了有关 n 个球放到 m 个盒子的各种不同条件下放球方法数的结果.

4. $$\left\{{n+1 \atop r}\right\} = \binom{n}{0}\left\{{0 \atop r-1}\right\} + \binom{n}{1}\left\{{1 \atop r-1}\right\} + \cdots + \binom{n}{n}\left\{{n \atop r-1}\right\}.$$

证明 等式左边计数了 $n+1$ 个不同的球放到 r 个相同的盒子

且不存在空盒的放球方法数. 对于其中的任意一种放法，拿出包含球 a_{n+1} 的盒子，就得到至多 n 个球放到 $r-1$ 个相同的盒子且不存在空盒的一种放法.

考虑等式右边. 对于任意的正整数 k，$0\leqslant k\leqslant n$，$\binom{n}{k}$ 表示从 n 个不同的球中任取 k 个球的选法数. 对于其中的任何一种选法，将这 k 个球恰好放到 $r-1$ 个相同的盒子的放法有 $\left\{ {k \atop r-1} \right\}$ 种，所以 $\binom{n}{k}\left\{ {k \atop r-1} \right\}$ 表示从 n 个不同的球中取 k 个恰好放到 $r-1$ 个相同的盒子的放法数. 如果对 k 求和，就得到至多 n 个不同的球恰好放到 $r-1$ 个相同的盒子的放法数，因此等式成立. ∎

表 8.2

球是否被标号	盒子是否标号	是否允许空盒	放球的方法数	所对应的组合问题
否	否	否	$P_m(n)-P_{m-1}(n)$	将 n 恰好剖分成 m 个部分的方法数
否	否	是	$P_m(n)$	将 n 剖分成 t 个部分($t\leqslant m$)的方法数
否	是	否	$\binom{n-1}{m-1}$	将 n 恰好剖分成 m 个有序的部分且允许重复的方法数
否	是	是	$\binom{n+m-1}{n}$	方程 $x_1+x_2+\cdots+x_m=n$ 的非负整数解的个数
是	否	否	$\left\{ {n \atop m} \right\}$	第二类 Stirling 数
是	否	是	$\left\{ {n \atop 1} \right\}+\left\{ {n \atop 2} \right\}+\cdots+\left\{ {n \atop m} \right\}$	第二类 Stirling 数性质 3(1)
是	是	否	$m!\left\{ {n \atop m} \right\}$	第二类 Stirling 数性质 3(2)
是	是	是	m^n	第二类 Stirling 数性质 3(3)

5. 考虑第二类 Stirling 数的指数生成函数. 首先我们注意到

$$(e^x-1)^m=\left(x+\frac{x^2}{2!}+\cdots\right)^m=\sum_{n=0}^{\infty}a_n\frac{x^n}{n!},\qquad ①$$

其中

$$a_n=\sum\frac{n!}{n_1!\,n_2!\cdots n_m!},$$

求和是对方程 $n_1+n_2+\cdots+n_m=n$ 的一切正整数解来求. 根据第二类 Stirling 数的性质 3(2) 有

$$a_n=\begin{cases}0, & n<m,\\ \displaystyle\sum\frac{n!}{n_1!\,n_2!\cdots n_m!}=\sum\binom{n}{n_1\,n_2\cdots n_m}=m!\left\{\begin{matrix}n\\m\end{matrix}\right\}, & n\geqslant m.\end{cases}$$

将这个结果代入 ① 式得

$$(e^x-1)^m=\sum_{n=m}^{\infty}m!\left\{\begin{matrix}n\\m\end{matrix}\right\}\frac{x^n}{n!}.$$

可以近似地将$(e^x-1)^m$看成$\left\{\begin{matrix}n\\m\end{matrix}\right\}$的指数生成函数,只不过相差$m!$倍罢了. 用二项式定理将$(e^x-1)^m$ 展开得

$$\begin{aligned}
&(e^x-1)^m\\
=&\binom{m}{m}e^{mx}-\binom{m}{m-1}e^{(m-1)x}\\
&+\binom{m}{m-2}e^{(m-2)x}-\cdots+(-1)^m\binom{m}{0}\cdot 1\\
=&\binom{m}{m}\left(1+\frac{m}{1!}x+\frac{m^2}{2!}x^2+\cdots\right)\\
&-\binom{m}{m-1}\left(1+\frac{(m-1)}{1!}x+\frac{(m-1)^2}{2!}x^2+\cdots\right)\\
&+\binom{m}{m-2}\left(1+\frac{(m-2)}{1!}x+\frac{(m-2)^2}{2!}x^2+\cdots\right)\\
&-\cdots+(-1)^m\binom{m}{0}\cdot 1.
\end{aligned}$$

比较上式两边$\frac{x^n}{n!}$的系数得

$$m!\left\{\begin{matrix}n\\m\end{matrix}\right\}=\binom{m}{m}m^n-\binom{m}{m-1}(m-1)^n+\binom{m}{m-2}(m-2)^n-\cdots+(-1)^{m-1}\binom{m}{1}\cdot 1^n,$$

从而得到关于$\left\{\begin{matrix}n\\m\end{matrix}\right\}$的恒等式

$$\left\{\begin{matrix}n\\m\end{matrix}\right\}=\frac{1}{m!}\left[\binom{m}{m}m^n-\binom{m}{m-1}(m-1)^n+\binom{m}{m-2}(m-2)^n-\cdots+(-1)^{m-1}\binom{m}{1}\cdot 1^n\right].$$

通过这个恒等式也可以计算$\left\{\begin{matrix}n\\m\end{matrix}\right\}$. 例如

$$\left\{\begin{matrix}5\\2\end{matrix}\right\}=\frac{1}{2!}\left[\binom{2}{2}2^5-\binom{2}{1}1^5\right]=\frac{1}{2}(32-2)=15,$$

$$\left\{\begin{matrix}4\\2\end{matrix}\right\}=\frac{1}{2!}\left[\binom{2}{2}2^4-\binom{2}{1}1^4\right]=\frac{1}{2}(16-2)=7.$$

习　题　八

1. 设 $f(n)$ 是 Fibonacci 数，计算

$$f(0)-f(1)+f(2)-\cdots+(-1)^n f(n).$$

2. 证明以下关于 Fibonacci 数的恒等式

(1) $f^2(n-1)+f^2(n)=f(2n)$;

(2) $f(n)\cdot f(n+1)-f(n-1)\cdot f(n-2)=f(2n)$;

(3) $f^3(n)+f^3(n+1)-f^3(n-1)=f(3n+2)$.

3. 设 $f(n)$ 是 Fibonacci 数，

(1) 证明 $f(n)\cdot f(n+2)-f^2(n+1)=\pm 1$;

(2) 当 n 是什么值时，等式右边是 1？当 n 是什么值时，等式右边是 -1？

4. 设级数 $\{H_n\}$ 满足 $H_1=a$, $H_2=b$，且 $H_{n+2}=H_{n+1}+H_n$，求 H_n.

5. 已知 $a_0=0$，$a_1=1$，$a_2=4$，$a_3=12$ 满足递推方程 $a_n+c_1a_{n-1}+c_2a_{n-2}=0$，求 c_1 和 c_2。

6. 求解递推方程：

(1) $\begin{cases} a_n-7a_{n-1}+12a_{n-2}=0, \\ a_0=4,\ a_1=6; \end{cases}$

(2) $\begin{cases} a_n+a_{n-2}=0, \\ a_0=0,\ a_1=2; \end{cases}$

(3) $\begin{cases} a_n+6a_{n-1}+9a_{n-2}=3, \\ a_0=0,\ a_1=1; \end{cases}$

(4) $\begin{cases} a_n-3a_{n-1}+2a_{n-2}=1, \\ a_0=4,\ a_1=6; \end{cases}$

(5) $\begin{cases} a_n-7a_{n-1}+10a_{n-2}=3^n, \\ a_0=0,\ a_1=1. \end{cases}$

7. 已知递推方程 $c_0a_n+c_1a_{n-1}+c_2a_{n-2}=f(n)$ 的解是 3^n+4^n+2，若对所有的 n 有 $f(n)=6$，求 c_0，c_1 和 c_2。

8. 求解递推方程：

(1) $\begin{cases} na_n+(n-1)a_{n-1}=2^n, & n\geqslant 1, \\ a_0=273; \end{cases}$

(2) $\begin{cases} a_n-na_{n-1}=n!, & n\geqslant 1, \\ a_0=2. \end{cases}$

9. 设 a_n 是 n 个元素的集合的划分个数，证明

$$a_{n+1}=\sum_{i=0}^{\infty}\binom{n}{i}a_i, \qquad a_0=1.$$

10. 设 a_n 为一凸 n 边形被其对角线划分为互不重合的区域个数，设该凸 n 边形每三条对角线都不交于一点.

(1) 证明

$$\begin{cases} a_n-a_{n-1}=\dfrac{(n-1)(n-2)(n-3)}{6}+n-2, & n\geqslant 3, \\ a_0=a_1=a_2=0; \end{cases}$$

(2) 求 a_n.

11. 求下列 n 阶行列式的值 d_n，

$$d_n = \begin{vmatrix} 2 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 2 & \cdots & 0 & 0 \\ \cdots & & & & & \\ 0 & 0 & 0 & \cdots & 1 & 2 \end{vmatrix}.$$

12. 平面上有 n 条直线，它们两两相交且没有三线交于一点，问这 n 条直线把平面分成多少个区域？

13. 一个 $1 \times n$ 的方格图形用红、蓝两色涂色每个方格. 如果每个方格只能涂一种颜色，且不允许两个红格相邻，问有多少种涂色方案？

14. 设 $f(n,k)$ 是从集合 $\{1,2,\cdots,n\}$ 中选出的没有两个连续整数的 k-子集个数.

(1) 给出 $f(n,k)$ 满足的递推方程；

(2) 证明 $f(n,k) = \binom{n-k+1}{k}$；

(3) 证明 $\{1,2,\cdots,n\}$ 的不含两个连续整数的所有子集个数是 Fibonacci 数 $f(n+2)$.

15. 在图 8.8 的长方形中，$AC/AB = (1+\sqrt{5})/2$. 作线段 EF，使 $ABFE$ 是一个正方形，证明长方形 $EFDC$ 和 $ACDB$ 相似. 如果重复这个过程，就得到图 8.8 中的图形. 证明每一步得到的长方形都和原来的长方形相似.

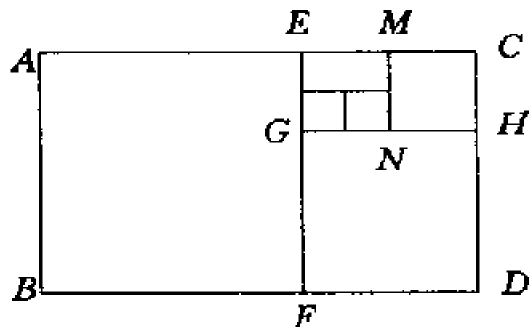


图 8.8

16. 证明生成函数的性质 2,5,8 和 10.

17. 确定数列 $\{a_n\}$ 的生成函数.

(1) $a_n = (-1)^n(n+1)$；

(2) $a_n = (-1)^n 2^n$；

(3) $a_n = n+5$；

(4) $a_n = \binom{n}{3}$.

18. 设数列 $\{a_n\}$ 的生成函数为 $A(x)$，试确定 a_n.

(1) $A(x)=\frac{x(1+x)}{(1-x)^3}$;

(2) $A(x)=\frac{1}{(1-x)(1-x^2)}$.;

19. 设多重集 $S=\{\infty\cdot a_1,\infty\cdot a_2,\infty\cdot a_3,\infty\cdot a_4\}$，$c_n$ 是 S 的满足以下条件的 n-组合数，且数列 $\{c_n\}$ 的生成函数为 $C(x)$，求 $C(x)$.

(1) 每个 a_i 出现奇数次，$i=1,2,3,4$；

(2) 每个 a_i 出现 3 的倍数次，$i=1,2,3,4$；

(3) a_1 不出现，a_2 至多出现 1 次；

(4) a_1 出现 1、3 或 11 次，a_2 出现 2、4 或 5 次；

(5) 每个 a_i 至少出现 10 次.

20. 一个 $1\times n$ 的方格图形用红、蓝、绿或橙四种颜色涂色. 如果有偶数个方格被涂成红色，还有偶数个方格被涂成绿色，问有多少种方案？

21. 证明正整数 N 被无序剖分成允许重复的正整数的方法数等于多重集 $\{N\cdot a\}$ 划分成子多重集的方法数.

22. 证明方程 $x_1+x_2+\cdots+x_7=13$ 和方程 $x_1+x_2+\cdots+x_{14}=6$ 有相同数目的非负整数解.

23. 设将 N 无序剖分成正整数之和且使得这些正整数都小于等于 m 的方法数为 $P(N,m)$，证明 $P(N,m)=P(N,m-1)+P(N-m,m)$.

24. 设 (N,n,m) 表示将 N 有序剖分成 n 个正整数且每个正整数都小于等于 m 的方案数，证明 (N,n,m) 就是 $(x+x^2+\cdots+x^m)^n$ 的展开式中 x^N 的系数.

25. 证明 N 的一种剖分（在这些剖分中仅仅奇数项是可以重复的）的个数等于 N 的另一种剖分（在这些剖分中没有一个项出现的次数大于 3）的个数.

26. 确定下面数列 $\{a_n\}$ 的指数生成函数.

(1) $a_n=n!$；

(2) $a_n=2^n\cdot n!$；

(3) $a_n=(-1)^n$.

27. 证明下面的等式：

(1) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{1}{m+k+1}=\frac{n!\,m!}{(n+m+1)!}$；

(2) $\sum_{k=0}^{n}\binom{n}{k}\binom{m+k}{m}^{-1}\frac{(-1)^k}{m+k+1}=\frac{1}{n+m+1}$.

28. 用三个 1、两个 2、五个 3 可以组成多少个不同的四位数?如果这个四位数是偶数,那么又有多少个?

29. 确定由 n 个奇数字组成的,并且 1 和 3 每个数字出现正偶数次的数的个数.

30. $2n$ 个点均匀分布在一个圆周上,若用 n 条不相交的弦将这 $2n$ 个点配成 n 对,证明不同的配对方法数是第 $n+1$ 个 Catalan 数 $\frac{1}{n+1}\binom{2n}{n}$. 例如图 8.9 就给出了 8 个点的一种配对方案.

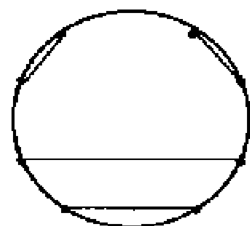


图 8.9

31. 计算 $\begin{bmatrix}6\\n\end{bmatrix}$,其中 $n=1,2,3,4,5,6$.

32. 计算 $\begin{bmatrix}7\\n\end{bmatrix}$,其中 $n=1,2,3,4,5,6,7$.

33. 证明 $n!=\begin{bmatrix}n\\n\end{bmatrix}n^n-\begin{bmatrix}n\\n-1\end{bmatrix}n^{n-1}+\begin{bmatrix}n\\n-2\end{bmatrix}n^{n-2}-\cdots$.

34. 用恰好 k 种可能的颜色做旗子,使得每面旗子由 n 条彩带构成($n\geqslant k$),且相邻的两条彩带的颜色都不相同,证明不同的旗子数是 $k!\begin{Bmatrix}n-1\\k-1\end{Bmatrix}$.

35. 设 $T(n,t)$ 表示将 n 元集划分成 t 个非空有序子集的方法数. 证明 $T(n,t)=t!\begin{Bmatrix}n\\t\end{Bmatrix}$.

36. 设 b_n 表示把 n 元集划分成非空子集的方法数,我们称 b_n 为 Bell 数. 证明

(1) $b_n=\binom{n-1}{0}b_0+\binom{n-1}{1}b_1+\cdots+\binom{n-1}{n-1}b_{n-1}$;

(2) $b_n=\begin{Bmatrix}n\\1\end{Bmatrix}+\begin{Bmatrix}n\\2\end{Bmatrix}+\cdots+\begin{Bmatrix}n\\n\end{Bmatrix}$.

第九章　组合计数定理

本章主要介绍两个组合计数定理——包含排斥原理和Polya定理及其应用.

§9.1　包含排斥原理

设S为有穷集,A是S的子集,若把A相对于S的补集记作$\overline{A}$,则有

$$|\overline{A}| = |S| - |A|.$$

设P_1,P_2是两种性质,A_1和A_2分别表示S中具有性质P_1和性质P_2的元素构成的子集,则有

$$|\overline{A}_1 \cap \overline{A}_2| = |S| - |A_1| - |A_2| + |A_1 \cap A_2|.$$

这两个等式都是**包含排斥原理**的简单形式.

一般说来,设S为有穷集,$P_1,P_2,\cdots,P_m$是m种性质,且A_i是S中具有性质P_i的元素构成的子集,$i=1,2,\cdots,m$.这时包含排斥原理可叙述为:

定理 9.1　S中不具有性质$P_1,P_2,\cdots$和P_m的元素数是

$$|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| = |S| - \sum_{i=1}^{m}|A_i| + \sum_{1\leqslant i<j\leqslant m}|A_i \cap A_j|$$
$$- \sum_{1\leqslant i<j<k\leqslant m}|A_i \cap A_j \cap A_k| + \cdots + (-1)^m|A_1 \cap A_2 \cap \cdots \cap A_m|.$$

证　等式左边是S中不具有性质$P_1,P_2,\cdots,P_m$的元素数.我们将要证明,对S中的任何一个元素x,如果x不具有性质$P_1,P_2,\cdots,P_m$,则对等式右边的贡献是1;如果x至少具有其中的一条性质,则对等式右边的贡献是0.

设x不具有性质$P_1,P_2,\cdots,P_m$,即$\forall i \in \{1,2,\cdots,m\}, x \notin A_i$.令$T=\{1,2,\cdots,m\}$,对$T$的所有2-组合$\{i,j\}$都有$x \notin A_i \cap A_j$,对$T$

的所有3-组合$\{i,j,k\}$都有$x \notin A_i \cap A_j \cap A_k, \cdots$，直到$x \notin A_1 \cap A_2 \cap \cdots \cap A_m$. 但$x \in S$，所以它对等式右边的贡献是

$$1 - 0 + 0 - 0 + \cdots + (-1)^m 0 = 1.$$

设x具有n条性质，$1 \leqslant n \leqslant m$，则$x$对$|S|$的贡献是1，对$\sum_{i=1}^{m}|A_i|$的贡献是$n = \binom{n}{1}$，对$\sum_{1 \leqslant i < j \leqslant m}|A_i \cap A_j|$的贡献为$\binom{n}{2}, \cdots$，对$|A_1 \cap A_2 \cap \cdots \cap A_m|$的贡献为$\binom{n}{m}$，所以$x$对等式右边的总贡献是

$$\begin{aligned} & \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^m \binom{n}{m} \\ = & \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0. \end{aligned}$$ ∎

推论 S中至少具有一条性质的元素数是

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{i=1}^{m}|A_i| - \sum_{1 \leqslant i < j \leqslant m}|A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant m}|A_i \cap A_j \cap A_k| - \cdots + (-1)^{m+1}|A_1 \cap A_2 \cap \cdots \cap A_m|.$$

证明
$$\begin{aligned} & |A_1 \cup A_2 \cup \cdots \cup A_m| \\ = & |S| - |\overline{A_1 \cup A_2 \cup \cdots \cup A_m}| \\ = & |S| - |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| \\ = & \sum_{i=1}^{m}|A_i| - \sum_{1 \leqslant i < j \leqslant m}|A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant m}|A_i \cap A_j \cap A_k| - \cdots \\ & + (-1)^{m+1}|A_1 \cap A_2 \cap \cdots \cap A_m|. \end{aligned}$$ ∎

【例9.1】 求在1和1000之间(包括1和1000在内)不能被5、6和8整除的数的个数.

解 令P_1, P_2, P_3分别表示一个整数能被5、6或8整除的性质. 设

$$S = \{x \mid x\text{是整数且}1 \leqslant x \leqslant 1000\},$$

$$A_i = \{x \mid x \in S \text{ 且 } x \text{ 具有性质 } P_i\},\ i = 1,2,3.$$

则有下面的结果：

$$|A_1| = [1000/5] = 200,$$
$$|A_2| = [1000/6] = 166,$$
$$|A_3| = [1000/8] = 125,$$
$$|A_1 \cap A_2| = [1000/[5,6]] = [1000/30] = 33,$$
$$|A_1 \cap A_3| = [1000/[5,8]] = [1000/40] = 25,$$
$$|A_2 \cap A_3| = [1000/[6,8]] = [1000/24] = 41,$$
$$|A_1 \cap A_2 \cap A_3| = [1000/[5,6,8]] = [1000/120] = 8.$$

由定理 9.1 得

$$|\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3|$$
$$= 1000 - (200 + 166 + 125) + (33 + 25 + 41) - 8 = 600.$$

【例 9.2】 证明以下等式

$$\binom{n-m}{r-m} = \binom{m}{0}\binom{n}{r} - \binom{m}{1}\binom{n-1}{r} + \cdots$$
$$+ (-1)^m \binom{m}{m}\binom{n-m}{r},$$

其中 n,r,m 为正整数，$m \leqslant r \leqslant n$.

证 令 $S = \{1,2,\cdots,n\}$，$A = \{1,2,\cdots,m\}$. 等式左边表示从 S 中选取包含 A 的 r- 子集的方法数 N. 设 P_j 表示在 S 的 r- 子集中不包含 j 的性质，$j = 1,2,\cdots,m$，A_j 是具有性质 P_j 的 S 的 r- 子集的集合，则

$$|A_j| = \binom{n-1}{r},\quad 1 \leqslant j \leqslant m,$$
$$|A_i \cap A_j| = \binom{n-2}{r},\quad 1 \leqslant i < j \leqslant m,$$

……………………………………………

$$|A_1 \cap A_2 \cap \cdots \cap A_m| = \binom{n-m}{r}.$$

由定理 9.1 得

$$N=|\overline{A}_1\cap\overline{A}_2\cap\cdots\cap\overline{A}_m|$$
$$=\binom{n}{r}-\binom{m}{1}\binom{n-1}{r}+\binom{m}{2}\binom{n-2}{r}$$
$$-\cdots+(-1)^m\binom{m}{m}\binom{n-m}{r}$$
$$=\binom{m}{0}\binom{n}{r}-\binom{m}{1}\binom{n-1}{r}+\binom{m}{2}\binom{n-2}{r}$$
$$-\cdots+(-1)^m\binom{m}{m}\binom{n-m}{r}.$$ ∎

使用包含排斥原理可以解决许多组合计数问题，如多重集的 r-组合数，不定方程的整数解的个数等.

设多重集 $S=\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$. 如果某个 $n_i>r$，我们可以用 r 来代替 n_i 得到多重集 S'. 不难看出 S' 的 r-组合数就是 S 的 r-组合数，所以不妨假设所有的 $n_i\leqslant r, i=1,2,\cdots,k$. 下面举例说明怎样用包含排斥原理来求 S 的 r-组合数.

【例 9.3】 确定多重集 $S=\{3\cdot a,\ 4\cdot b,\ 5\cdot c\}$ 的 10-组合数.

解 令 $T=\{\infty\cdot a,\infty\cdot b,\infty\cdot c\}$，$T$ 的所有 10-组合构成集合 W，由定理 7.6 得

$$|W|=\binom{3+10-1}{10}=\binom{12}{10}=\binom{12}{2}=66.$$

任取 T 的一个 10-组合，如果其中的 a 多于 3 个，则称它具有性质 P_1；如果其中的 b 多于 4 个，则称它具有性质 P_2；如果其中的 c 多于 5 个，则称它具有性质 P_3. 令

$A_i=\{x\,|\,x\in W$ 且 x 具有性质 $P_i\}$，$i=1,2,3$，则所求的 10-组合数即 $|\overline{A_1}\cap\overline{A_2}\cap\overline{A_3}|$.

先计算 $|A_1|$，$|A_2|$ 和 $|A_3|$. A_1 中的每个 10-组合至少含有 4 个 a，把这 4 个 a 拿走就得到 T 的一个 6-组合. 反之，对 T 的任意一个 6-组合加上 4 个 a 就得到 A_1 中的一个10-组合，所以 $|A_1|$ 就是 T 的

6-组合数,即

$$|A_1| = \binom{3+6-1}{6} = \binom{8}{6} = \binom{8}{2} = 28.$$

同理可得

$$|A_2| = \binom{3+5-1}{5} = \binom{7}{5} = \binom{7}{2} = 21,$$

$$|A_3| = \binom{3+4-1}{4} = \binom{6}{4} = \binom{6}{2} = 15.$$

用类似的方法可以得到下面的结果:

$$|A_1 \cap A_2| = \binom{3+1-1}{1} = 3,$$

$$|A_1 \cap A_3| = \binom{3+0-1}{0} = 1,$$

$$|A_2 \cap A_3| = 0,$$

$$|A_1 \cap A_2 \cap A_3| = 0.$$

从而有

$$|\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3|$$
$$= 66 - (28 + 21 + 15) + (3 + 1 + 0) - 0 = 6.$$

这与用生成函数方法求解的结果是一致的(见例 8.25).

【例 9.4】 确定方程

$$\begin{cases} x_1 + x_2 + x_3 = 5, \\ 0 \leqslant x_1 \leqslant 2,\ 0 \leqslant x_2 \leqslant 2,\ 1 \leqslant x_3 \leqslant 5 \end{cases}$$

的整数解的个数.

解 令 $x'_3 = x_3 - 1$,代入原方程得

$$\begin{cases} x_1 + x_2 + x'_3 = 4, \\ 0 \leqslant x_1 \leqslant 2,\ 0 \leqslant x_2 \leqslant 2,\ 0 \leqslant x'_3 \leqslant 4. \end{cases}$$

不难看到该方程的整数解个数就是原方程的整数解个数,也是多重集 $S = \{2 \cdot a, 2 \cdot b, 4 \cdot c\}$ 的 4-组合数.仿照例 9.3 的方法求得 S 的 4-组合数,结果得 9.而原方程的 9 个整数解 (x_1, x_2, x_3) 是 $(0,0,5)$,

(0,1,4),(0,2,3),(1,0,4),(1,1,3),(1,2,2),(2,0,3),(2,1,2),(2,2,1).

【例 9.5】 设 n 是正整数,$n \geqslant 2$,欧拉函数 $\phi(n)$ 表示小于等于 n 且与 n 互质的正整数个数. 求 $\phi(n)$ 的表达式.

解 对于任意给定的正整数 $n, n \geqslant 2$,都有如下的分解式

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

其中 $p_1, p_2, \cdots, p_k$ 为素数,$\alpha_1, \alpha_2, \cdots, \alpha_k$ 为正整数. 令

$$S = \{x \mid x \text{ 是小于等于 } n \text{ 的正整数}\},$$

$$A_i = \{x \mid x \in S \text{ 且 } p_i \text{ 整除 } x\},\ i = 1, 2, \cdots, k.$$

则有以下结果:

$$|S| = n,$$

$$|A_i| = [n/p_i] = \frac{n}{p_i}, \qquad i = 1, 2, \cdots, k,$$

$$|A_i \cap A_j| = [n/[p_i, p_j]] = \frac{n}{p_i p_j}, \qquad 1 \leqslant i < j \leqslant k,$$

……………………………………

$$|A_1 \cap A_2 \cap \cdots \cap A_k| = [n/[p_1, p_2, \cdots, p_k]] = \frac{n}{p_1 p_2 \cdots p_k}.$$

由定理 9.1 得

$$\begin{aligned}
\phi(n) &= |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_k| \\
&= n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{1 \leqslant i < j \leqslant k} \frac{n}{p_i p_j} - \cdots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k} \\
&= n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k}\right) + n\left(\frac{1}{p_1 p_2} + \cdots + \frac{1}{p_{k-1} p_k}\right) \\
&\quad - \cdots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k} \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

例如 $30 = 2 \times 3 \times 5$,则

$$\phi(30) = 30 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8,$$

小于等于 30 且与 30 互质的正整数有 8 个，即 1，7，11，13，17，19，23 和 29.

下面考虑包含排斥原理的推广形式. 为了书写方便，引入下述符号：

$$W(0) = |S|,$$

$$W(1) = \sum_{i=1}^{m} |A_i|,$$

$$W(2) = \sum_{1 \leqslant i < j \leqslant m} |A_i \cap A_j|,$$

$$W(3) = \sum_{1 \leqslant i < j < k \leqslant m} |A_i \cap A_j \cap A_k|,$$

$$\cdots\cdots\cdots\cdots$$

$$W(m) = |A_1 \cap A_2 \cap \cdots \cap A_m|.$$

使用这些符号，定理 9.1 可以写作

$$\begin{aligned} &|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| \\ &= W(0) - W(1) + W(2) - \cdots + (-1)^m W(m) \\ &= \sum_{t=0}^{m} (-1)^t W(t), \end{aligned}$$

而推论则写作

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_m| &= W(1) - W(2) + \cdots + (-1)^{m+1} W(m) \\ &= \sum_{t=1}^{m} (-1)^{t+1} W(t). \end{aligned}$$

定理 9.2　设 S 为有穷集，$P_1, P_2, \cdots, P_m$ 是 m 条性质，A_i 是 S 中具有性质 P_i 的元素构成的子集，$i = 1, 2, \cdots, m$，则 S 中恰好具有 $r(0 \leqslant r \leqslant m)$ 条性质的元素数是

$$W(r) - \binom{r+1}{r} W(r+1) + \binom{r+2}{r} W(r+2)$$

$$- \cdots \pm \binom{m}{r} W(m)$$

$$=\sum_{t=0}^{m-r}(-1)^t\binom{r+t}{t}W(r+t).$$

证明 任取 $x\in S$，若 x 具有的性质数少于 r，则 x 对公式的各项贡献为0. 若 x 恰好具有 r 条性质，则 x 对 $W(r)$ 项贡献为1，而对以后各项贡献都是0，所以 x 对公式的总贡献是1. 若 x 恰好具有 $r+k$ 条性质，$k=1,2,\cdots,m-r$，则 x 对公式中的 $W(r+j)$ 项的贡献为 $\binom{r+k}{r+j}$，其中 $j=0,1,\cdots,k$，而对以后的各项贡献为0，因而 x 对公式的总贡献是

$$\begin{aligned}
&\sum_{j=0}^{k}(-1)^j\binom{r+j}{r}\binom{r+k}{r+j}\\
&=\sum_{j=0}^{k}(-1)^j\binom{r+k}{r}\binom{k}{j} \quad \text{(根据 7.8 式)}\\
&=\binom{r+k}{r}\sum_{j=0}^{k}(-1)^j\binom{k}{j}\\
&=0. \quad \text{(根据 7.5 式)}
\end{aligned}$$

综上所述，公式计数了 S 中恰好具有 r 条性质的元素. ▮

定理9.2是包含排斥原理的推广形式，当 $r=0$ 时公式变成

$$\sum_{t=0}^{m}(-1)^t\binom{t}{t}W(t)=\sum_{t=0}^{m}(-1)^tW(t),$$

这就是包含排斥原理(定理9.1).

【例9.6】 对24名科技人员进行掌握外语情况的调查，其统计资料如下：每个人至少会一门外语，其中会英、日、德和法语的人数分别是13，5，10和9人，会英语和日语两种语言的有2人，会英语和德语、英语和法语、德语和法语的各有4人. 如果会日语的人既不懂法语也不懂德语，问只会一种语言的有多少人？会英、德和法语三种语言的有多少人？

解 设 S 是24名科技人员构成的集合，A_1,A_2,A_3 和 A_4 分别代

表其中会英语、日语、德语和法语的人构成的子集，由题意不难得到

$$|A_1| = 13,\ |A_2| = 5,\ |A_3| = 10,\ |A_4| = 9,$$
$$|A_1 \cap A_2| = 2,\ |A_1 \cap A_3| = 4,\ |A_1 \cap A_4| = 4,$$
$$|A_2 \cap A_3| = 0,\ |A_2 \cap A_4| = 0,\ |A_3 \cap A_4| = 4,$$
$$|A_1 \cap A_2 \cap A_3 \cap A_4| = 0,$$
$$|A_1 \cap A_2 \cap A_3| = 0,\ |A_1 \cap A_2 \cap A_4| = 0,\ |A_2 \cap A_3 \cap A_4| = 0,$$
$$W(1) = |A_1| + |A_2| + |A_3| + |A_4| = 37,$$
$$W(2) = \sum_{1 \leqslant i < j \leqslant 4} |A_i \cap A_j| = 2 + 4 + 4 + 4 = 14,$$
$$W(3) = |A_1 \cap A_3 \cap A_4|,$$
$$W(4) = 0.$$

由定理 9.1 的推论有

$$W(1) - W(2) + W(3) - W(4) = 24,$$

解得 $W(3) = 1$，即 $|A_1 \cap A_3 \cap A_4| = 1$. 又由定理 9.2 知道只会一种语言的人数是

$$\begin{aligned} & W(1) - \binom{2}{1}W(2) + \binom{3}{2}W(3) - \binom{4}{3}W(4) \\ = & 37 - 2 \times 14 + 3 \times 1 - 4 \times 0 \\ = & 12. \end{aligned}$$

【例 9.7】 证明组合恒等式

$$\sum_{i=n}^{m} (-1)^{i-n} \binom{m}{i} \binom{i}{n} = 0,$$

其中 $m, n \in Z^+, n < m$.

证 令 $S = \{a\}$，且 a 具有 m 条性质，则有

$$W(i) = \binom{m}{i}, \quad i = n, n+1, \cdots, m.$$

又知 S 中具有 n 条性质的元素数为 0，由定理 9.2 得

$$\sum_{t=0}^{m-n} (-1)^t \binom{n+t}{t} W(n+t) = 0.$$

将 $t = i - n$ 和 $W(i) = \binom{m}{i}$ 依次代入得

$$\sum_{i=n}^{m}(-1)^{i-n}\binom{i}{i-n}\binom{m}{i} = 0,$$

即

$$\sum_{i=n}^{m}(-1)^{i-n}\binom{m}{i}\binom{i}{n} = 0. \quad \blacksquare$$

§9.2 对称筛公式及应用

考虑上一节的定理 9.1，若 m 种性质是对称的，即对任意给定的正整数 k，$1 \leqslant k \leqslant m-1$，任意选择 k 种性质 $P_{i_1}, P_{i_2}, \cdots, P_{i_k}$，具有这些性质的元素数仅与 k 的大小有关，而与这 k 种性质的选择无关. 例如

$k = 1$，有 $|A_1| = |A_2| = \cdots = |A_m| = N_1$，

$k = 2$，有 $|A_1 \cap A_2| = |A_1 \cap A_3| = \cdots = |A_{m-1} \cap A_m| = N_2$，

$k = 3$，有 $|A_1 \cap A_2 \cap A_3| = |A_1 \cap A_2 \cap A_4| = \cdots$
$= |A_{m-2} \cap A_{m-1} \cap A_m| = N_3$，

…………………………………………

$k = m-1$，有 $|A_1 \cap A_2 \cap \cdots \cap A_{m-1}| = \cdots$
$= |A_2 \cap A_3 \cap \cdots \cap A_m| = N_{m-1}$.

此外，又将 $|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m|$ 记为 N_0，$|S|$ 记为 N，$|A_1 \cap A_2 \cap \cdots \cap A_m|$ 记为 N_m，则定理 9.1 中的公式表示为

$$\begin{aligned} N_0 &= N - \binom{m}{1}N_1 + \binom{m}{2}N_2 - \cdots \pm \binom{m}{m}N_m \\ &= N + \sum_{t=1}^{m}(-1)^t\binom{m}{t}N_t. \end{aligned}$$

这个公式称作**对称筛公式**，它在组合计数问题中有着广泛的应用，如错位排列，有限制条件的排列和有禁区排列的计数.

考虑下面的例子，在书架上有 5 本书，把它们全拿下来，然后再

可以证明 D_n 满足下面的递推方程：

$$\begin{cases} D_n = (n-1)(D_{n-2} + D_{n-1}), & n \geqslant 3, \\ D_1 = 0,\ D_2 = 1. \end{cases}$$

考虑排列 $12\cdots n$ 的所有的错位排列. 根据第一位数字是 2,3,…,或 n 将它们划分成 $n-1$ 类. 显然每一类的错位排列数相等，令 d_n 表示第一位是 2 的错位排列数，则

$$D_n = (n-1)d_n.$$

考虑所有形为 $2i_2i_3\cdots i_n$ 的错位排列，将它们划分成两个子类，称 $i_2 = 1$ 的为第一子类，并把其中的排列个数记作 d'_n，称 $i_2 \neq 1$ 的为第二子类，个数记为 d''_n，那么有

$$d_n = d'_n + d''_n = D_{n-2} + D_{n-1},$$

从而得到

$$D_n = (n-1)(D_{n-2} + D_{n-1}).$$

这是一个二阶递推方程，初值是 $D_1 = 0, D_2 = 1$. 回顾例 8.15，使用迭代归纳法，该方程的解是

$$D_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right].$$

这与用包含排斥原理求解的结果一致.

下面考虑另一类有限制条件的排列问题，就是对元素之间相邻关系加以限制的排列问题.

设 $X = \{1,2,\cdots,n\}$，在 X 的排列中不出现 $12,23,\cdots,(n-1)n$ 的排列称为**有限制条件的排列**. 有限制条件的排列数记作 Q_n.

当 $n = 1$ 时，$Q_1 = 1$. 当 $n = 2$ 时，满足条件的排列是 21，所以 $Q_2 = 1$. 当 $n = 3$ 时，满足条件的排列有 213,321,132，即 $Q_3 = 3$. 当 $n = 4$ 时，满足条件的排列有 4132,4321,4213,3214,3241,3142,2431,2413,2143,1324,1432，即 $Q_4 = 11$.

对于一般的正整数 n，有下面的定理.

定理 9.4　设 n 是正整数，则

$$= 24 \times \frac{12 - 4 + 1}{24} = 9.$$

$$D_5 = 5!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!}\right]$$

$$= 120 \times \frac{60 - 20 + 5 - 1}{120} = 44.$$

【例 9.8】

（1）重新排列 123456789，使得偶数在原来的位置上而奇数不在原来的位置上，问有多少种排法？

（2）如果要求只有 4 个数在原来的位置上，那么又有多少种排法？

解　（1）这种排列相当于 13579 的错位排列，由定理 9.3 有

$$D_5 = 5!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!}\right] = 44.$$

（2）从 $\{1,2,\cdots,9\}$ 中任取 4 个数的取法为 $\binom{9}{4}$，而其它 5 个数的错位排列数是 D_5，由乘法法则所求的排列数是

$$\binom{9}{4} D_5 = 126 \times 44 = 5544.$$

当 n 足够大时，错位排列出现的概率大约为 $\frac{1}{e}$. 由

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots$$

得

$$e^{-1} = \frac{D_n}{n!} + (-1)^{n+1}\frac{1}{(n+1)!} + (-1)^{n+2}\frac{1}{(n+2)!} + \cdots,$$

即

$$\left|e^{-1} - \frac{D_n}{n!}\right| < \frac{1}{(n+1)!}.$$

当 n 足够大时错位排列的概率 $\frac{D_n}{n!} \sim e^{-1}$.

下面让我们考虑有禁区的排列问题. 先介绍棋盘多项式的概念.

设 C 是一个棋盘(大小一致的正方形方格相邻接构成的图形), $r_k(C)$ 表示把 k 个相同的棋子布到 C 中的方案数. 在布棋时任意两个棋子不允许落到棋盘的同一行和同一列.

例如

r_1 (□)$=1$,

r_1 (⊟)$=r_1$(□□)$=r_1$(⧉)$=2$,

r_2 (⊟)$=r_2$(□□)$=0$,

r_2 (⧉)$=1$.

我们规定,对任意的棋盘 C 有 $r_0(C)=1$. 不难证明布棋方案数具有下面的性质:

1. 对于任意的棋盘 C 和正整数 k,如果 k 大于 C 中的方格数,则 $r_k(C)=0$.

2. $r_1(C)$ 等于 C 中的方格数.

3. 设 C_1 和 C_2 是两个棋盘,若 C_1 经过旋转或翻转就变成了 C_2,则 $r_k(C_1)=r_k(C_2)$.

4. 设 C_i 是从棋盘 C 中去掉指定的方格所在的行和列以后剩余的棋盘,C_l 是从棋盘 C 中去掉指定的方格以后剩余的棋盘,则有

$$r_k(C)=r_{k-1}(C_i)+r_k(C_l),\quad k\geqslant 1.$$

5. 设棋盘 C 由两个子棋盘 C_1 和 C_2 构成,如果 C_1 和 C_2 不存在公共的行和列,则

$$r_k(C)=\sum_{i=0}^{k} r_i(C_1)r_{k-i}(C_2).$$

定义 9.1 设 C 是棋盘,则

$$R(C)=\sum_{k=0}^{\infty} r_k(C)x^k$$

叫做**棋盘多项式**.

$$Q_n = n! - \binom{n-1}{1}(n-1)! + \binom{n-1}{2}(n-2)! - \cdots + (-1)^{n-1}\binom{n-1}{n-1}\cdot 1!.$$

证 设 $X = \{1,2,\cdots,n\}$，$S = \{x \mid x$ 是 X 的排列$\}$. 令 $A_j = \{x \mid x \in S$ 且 $j(j+1)$ 出现在 x 中$\}$，$j = 1,2,\cdots,n-1$. 不难证明

$$|A_j| = (n-1)! = N_1.$$

考虑 $|A_i \cap A_j|$，若排列 $x \in A_i \cap A_j$，则 $i(i+1)$，$j(j+1)$ 都出现在 x 中. 如果 $i+1 = j$，则 $i(i+1)(i+2)$ 可看成一个元素，相当于 $n-2$ 个元素的排列，即 $|A_i \cap A_j| = (n-2)!$. 如果 $i+1 \neq j$，则 $i(i+1)$，$j(j+1)$ 各看成一个元素，也相当于 $n-2$ 个元素的排列，$|A_i \cap A_j|$ 也是 $(n-2)!$. 因此有

$$N_2 = |A_i \cap A_j| = (n-2)!.$$

类似的分析可以得到：对任意的 $1 \leqslant k \leqslant n-1$ 有

$$N_k = (n-k)!,$$

从而有

$$Q_n = n! - \binom{n-1}{1}(n-1)! + \binom{n-1}{2}(n-2)! - \cdots + (-1)^{n-1}\binom{n-1}{n-1}\cdot 1!. \qquad \blacksquare$$

例如

$$\begin{aligned} Q_4 &= 4! - \binom{4-1}{1}(4-1)! + \binom{4-1}{2}(4-2)! \\ &\quad - \binom{4-1}{3}\cdot(4-3)! \\ &= 24 - 3 \times 3! + \binom{3}{2} \times 2! - \binom{3}{3}\cdot 1! \\ &= 24 - 18 + 6 - 1 \\ &= 11. \end{aligned}$$

制元素 i 不能排在第 j 个位置，则相应的布棋方案中棋盘的第 i 行第 j 列的方格不许放棋子. 所有不许放棋的方格构成了棋盘上的禁区.

定理 9.5　设 C 是 $n\times n$ 的具有给定禁区的棋盘，这个禁区对应于集合 $\{1,2,\cdots,n\}$ 中的元素在排列中不允许出现的位置，则这种有禁区的排列数是

$$n!-r_1(n-1)!+r_2(n-2)!-\cdots+(-1)^n r_n.$$

其中 r_i 是 i 个棋子布置到禁区的方案数.

证　先不考虑禁区的限制，那么 n 个棋子布到 $n\times n$ 棋盘上的方案有 $n!$ 个. 如果对 n 个棋子分别编号为 $1,2,\cdots,n$，并且认为编号不同的棋子放入同样的方格是不同的放置方案，那么带编号的棋子布到 $n\times n$ 棋盘上的方案数是 $n!\cdot n!$. 我们把这些方案构成的集合记作 S.

对 $j=1,2,\cdots,n$，令 P_j 表示第 j 个棋子落入禁区的性质，A_j 表示 S 中具有性质 P_j 的方案构成的子集. 易见这些性质具有对称性，根据乘法法则不难得到以下结果：

$$N_1=r_1(n-1)!(n-1)!,$$

$$N_2=2r_2(n-2)!(n-2)!,$$

$$\cdots\cdots\cdots\cdots$$

$$N_k=k!r_k(n-k)!(n-k)!,$$

$$\cdots\cdots\cdots\cdots$$

$$N_n=n!\cdot r_n.$$

由

$$\binom{n}{k}k!\cdot r_k(n-k)!(n-k)!=r_k(n-k)!n!,\quad k=1,2,\cdots,n$$

代入对称筛公式得

$$N_0=n!n!-r_1(n-1)!n!+r_2(n-2)!n!-\cdots+(-1)^n r_n\cdot n!.$$

由于带编号的布棋方案数与不带编号的布棋方案数相差 $n!$ 倍，因此所求的方案数是

实际上棋盘多项式 $R(C)$ 就是 C 中的布棋方案数序列 $\{r_k(C)\}$ 的生成函数.

例如

$$R(⧉) = r_0(⧉) + r_1(⧉)x + r_2(⧉)x^2 = 1 + x + x^2,$$
$$R(⊟) = r_0(⊟) + r_1(⊟)x + r_2(⊟)x^2 = 1 + 2x.$$

根据 $r_k(C)$ 的性质不难证明 $R(C)$ 的性质：

1. $R(C) = xR(C_i) + R(C_l)$，其中 C_i 和 C_l 的含义如前所述.
2. $R(C) = R(C_1) \cdot R(C_2)$，其中 C_1 和 C_2 的含义也如前所述.

这两条性质的证明留给读者完成.

【例 9.9】 计算 $R(⊞)$ 和 $R(⊞)$.

解 $R(⊠) = xR(□) + R(□□)$

$$= x(1 + x) + (1 + 2x)$$
$$= 1 + 3x + x^2,$$

$$R(⊠) = xR(⊠) + R(⊠)$$
$$= x[xR(⊟) + R(⊞)] + [xR(⊞) + R(⊞)]$$
$$= x[x(1 + 2x) + (1 + 3x + x^2)] + [x(1 + 3x + x^2)$$
$$+ R(⊞)]$$
$$= x(1 + 4x + 3x^2) + (x + 3x^2 + x^3 + 1 + 4x + 3x^2)$$
$$= 1 + 6x + 10x^2 + 4x^3.$$

下面我们就利用棋盘多项式来解决有禁区的排列问题. 首先可以看到 $X = \{1,2,\cdots,n\}$ 的一个排列恰好对应了 n 个棋子在 $n \times n$ 棋盘上的一种布棋方案. 在图 9.1，棋盘的行表示 X 中的元素，列表示排列中的位置，则这种布棋方案就对应了排列 2143. 如果在排列中限

	1	2	3	4
1		○		
2	○			
3				○
4			○	

图 9.1

$$D_n = n! - n(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^n \binom{n}{n} \cdot 0!$$

$$= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right].$$

最后让我们考虑一个二重错位排列问题.

【例 9.12】 家庭问题(Menage 问题) 有 n 对夫妻($n \geq 3$) 围圆桌就座. 如果要求男女相间且每对夫妻不能相邻,问有多少种方法? 称这个方法数为 Menage 数.

解 先让女士们间隔就座,就座的方法数是$(n-1)!$. 对于任何一种就座的方式,不妨将女士们依顺时针方向记为$\bar{1},\bar{2},\cdots,\bar{n}$. 令$\bar{i}$女士的丈夫为$i$,其中$i = 1,2,\cdots,n$,且将$\bar{i}$和$\overline{i+1}$女士之间的座位记为$i(i=1,2,\cdots,n-1)$,$\bar{n}$和$\bar{1}$女士之间的座位记为$n$. 假设男士们就座的顺序为$i_1 i_2 \cdots i_n$,则依题意必有$i_j \neq j, i_j \neq j+1(j=1,2,\cdots,n-1)$,且$i_n \neq n$, $i_n \neq 1$. 换句话说,要构成$\{1,2,\cdots,n\}$的排列$i_1 i_2 \cdots i_n$,且使得在下述阵列的每列中的元素都不相同.

$$\begin{matrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{matrix}$$

称排列$i_1 i_2 \cdots i_n$为**二重错位排列**. 设U_n是长为n的二重错位排列数,则 Menage 数恰好等于$(n-1)!U_n$.

设S是$\{1,2,\cdots,n\}$的所有排列的集合. 性质P_j表示在排列$i_1 i_2 \cdots i_n$中$i_j = j$或$i_j = j+1, j = 1,2,\cdots,n-1$,且$P_n$表示$i_n = n$或$i_n = 1$. 令$A_j = \{x \mid x \in S$且$x$具有性质$P_j\}$, $j = 1,2,\cdots,n$,则$U_n = |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n|$.

若排列$i_1 i_2 \cdots i_n$中有k个位置的数字满足$P_1,P_2,\cdots,P_n$中的k条性质,则其它的$n-k$个位置的数字有$(n-k)!$种选法. 依对称筛公式所求的排列数U_n似乎应该等于$n! + \sum_{k=1}^{n}(-1)^k\binom{n}{k}(n-k)!$. 但

$$n! - r_1(n-1)! + r_2(n-2)! - \cdots + (-1)^n r_n. \qquad \blacksquare$$

需要说明一点，这个定理适用于 $n \times n$ 棋盘的小禁区布棋问题. 如果是 $m \times n$ 的棋盘或者禁区很大的棋盘的布棋问题，那么只能直接用 $R(C)$ 来求解.

【例 9.10】 用四种颜色（红、蓝、绿、黄）涂染四台仪器 A,B,C 和 D. 规定每台仪器只能用一种颜色并且任意两台仪器都不能相同. 如果 B 不允许用蓝色和红色，C 不允许用蓝色和绿色，D 不允许用绿色和黄色，问有多少种染色方案？

解 这个问题就是图 9.2 中的有禁区的布棋问题. 禁区的棋盘多项式为

$$R(\square) = 1 + 6x + 10x^2 + 4x^3,$$

从而得到

$$r_1 = 6,\ r_2 = 10,\ r_3 = 4,\ r_4 = 0.$$

图 9.2

根据定理 9.5，所求的方案数是

$$\begin{aligned} N &= 4! - 6 \cdot 3! + 10 \cdot 2! - 4 \cdot 1! + 0 \\ &= 24 - 36 + 20 - 4 = 4. \end{aligned}$$

【例 9.11】 错位排列问题也可以看作是有禁区的排列问题，其禁区在主对角线上. 下面使用定理 9.5 来求 D_n.

解 禁区的棋盘多项式是

$$R\begin{pmatrix} \square & & \\ & \ddots & \\ & & \square \end{pmatrix} = \underbrace{R(\square) \cdot R(\square) \cdots \cdot R(\square)}_{n\text{个}} = (1+x)^n$$

$$= 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n,$$

从而得到

$$r_1 = n,\ r_2 = \binom{n}{2},\ \cdots,\ r_n = \binom{n}{n}.$$

根据定理 9.5 有

将对称筛公式中的$\binom{n}{k}$用$\dfrac{2n}{2n-k}\dbinom{2n-k}{k}$代替得到

$$U_n = n! + \sum_{k=1}^{n}(-1)^k \frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!,$$

而 Menage 数则等于$(n-1)!U_n$.

例如 3 对夫妻(A,a,B,b,C,c)安排就座应该有

$$\begin{aligned}(3-1)!U_3 &= 2!\left[3! - \frac{2\times 3}{2\times 3-1}\binom{2\times 3-1}{1}(3-1)!\right.\\ &\qquad + \frac{2\times 3}{2\times 3-2}\binom{2\times 3-2}{2}(3-2)!\\ &\qquad \left. - \frac{2\times 3}{2\times 3-3}\binom{2\times 3-3}{3}(3-3)!\right]\\ &= 2\times\left[3! - \frac{6}{5}\times 5\times 2 + \frac{6}{4}\binom{4}{2}\times 1 - 2\right]\\ &= 2\times(6-12+9-2)\\ &= 2\end{aligned}$$

种方式，就是图 9.3 中的方式.



图 9.3

§9.3 Burnside 引理

考虑下面的计数问题：把一个 2 × 2 的方格棋盘用黑或白两色涂色每个方格，如果棋盘可以随意转动，问有多少种不同的涂色方案？

请看图 9.4，如果棋盘固定不动，共有 $2^4 = 16$ 种不同的涂色方案. 但是当棋盘转动时，其中的一些方案可以变成另一些方案，如方案 3 逆时针转 90° 就变成方案 4. 同样的，方案 3 也可以变成方案 5 和

是由于性质$P_1,P_2,\cdots,P_n$并不是互相独立的，例如$i_1=2$时i_2不可能再等于2. 因此使得排列中有k个位置满足性质的方式不是$\binom{n}{k}$种. 我们不得不针对这种情况将对称筛公式做适当的修正. 考察下述$2n$个数的序列：

$$1,2,2,3,3,4,\cdots,n-1,n,n,1.$$

要从这个数列中选择k个不相邻的数，并且使得前后两个1不同时出现，易见这样的选法与排列$i_1i_2\cdots i_n$中有k个位置满足性质的方式是一一对应的. 设$a_1, a_2, \cdots, a_k$是上述序列中的k个不相邻的位置，则

$$1\leqslant a_1<a_2-1<a_3-2<\cdots$$
$$<a_k-(k-1)\leqslant 2n-(k-1),$$

即$\{a_1, a_2-1, a_3-2, \cdots, a_k-(k-1)\}$是集合$\{1, 2, \cdots, 2n-(k-1)\}$的一个$k$-组合. 反之，任给集合$\{1, 2, \cdots, 2n-(k-1)\}$的一个$k$-组合$\{b_1,b_2,\cdots,b_k\}$，其中

$$1\leqslant b_1<b_2<\cdots<b_k\leqslant 2n-(k-1),$$

则

$$\{b_1, b_2+1, b_3+2, \cdots, b_k+(k-1)\}$$

是$2n$个位置中的k个不相邻位置的一种选法. 因此，从$2n$个位置选取k个不相邻位置的方法数就是集合$\{1, 2, \cdots, 2n-(k-1)\}$的$k$-组合数$\binom{2n-(k-1)}{k}$. 下面要从这些选法中去掉位置1和位置$2n$同时出现的选法. 而位置1和位置$2n$同时被选中的选法相当于从位置$3, 4, \cdots, 2n-2$中选取$k-2$个不相邻位置的方法，即有

$$\binom{2n-4-(k-2-1)}{k-2}=\binom{2n-k-1}{k-2}$$

种方法. 因此所求的k种性质成立的方法数是

$$\binom{2n-(k-1)}{k}-\binom{2n-k-1}{k-2}=\frac{2n}{2n-k}\binom{2n-k}{k}.$$

$$E_1 = E_2 = \{1,2\},\ E_3 = E_4 = \{3,4\}.$$

定理 9.6　设 $N = \{1,2,\cdots,n\}$,G 是 N 上的置换群,对任意的 $k \in N$ 有

$$|Z_k| \cdot |E_k| = |G|.$$

证　任取 $k \in N$,设 $|E_k| = l$,即

$$E_k = \{a_1 = k,\ a_2,\cdots,a_l\},$$

其中 $a_i \in N, i = 1,2,\cdots,l$. 设置换

$$\sigma_i \in G, \text{且}\ \sigma_i(k) = a_i, i = 1,2,\cdots,l.$$

任取置换 $\tau \in Z_k$ 都有

$$\sigma_i\tau(k) = \sigma_i(\tau(k)) = \sigma_i(k) = a_i,\ i = 1,2,\cdots,l.$$

令

$$\sigma_i Z_k = \{\sigma_i\tau \mid \tau \in Z_k\},$$

则有

$$\sigma_1 Z_k \cup \sigma_2 Z_k \cup \cdots \cup \sigma_l Z_k \subseteq G,$$

并且对任意 $i,j \in \{1,2,\cdots,l\}, i \neq j$ 都有 $\sigma_i Z_k \cap \sigma_j Z_k = \varnothing$. 若不然,存在 $\sigma_i\tau_1 = \sigma_j\tau_2 \in \sigma_i Z_k \cap \sigma_j Z_k$,则有

$$\sigma_i\tau_1(k) = \sigma_j\tau_2(k) \Rightarrow \sigma_i(k) = \sigma_j(k) \Rightarrow a_i = a_j,$$

与 $a_i \neq a_j (i \neq j)$ 矛盾.

另一方面,对任意的 $\sigma \in G$,假设 $\sigma(k) = v \in N$,由 E_k 的定义可知 $v \in E_k$,即存在 $a_j \in E_k$,使 $a_j = v$. 又由于 $\sigma_j(k) = a_j$,因此有

$$\sigma_j^{-1}\sigma(k) = \sigma_j^{-1}(\sigma(k)) = \sigma_j^{-1}(a_j) = k.$$

从而证明了 $\sigma_j^{-1}\sigma \in Z_k$,即 $\sigma \in \sigma_j Z_k$. 这就推出

$$G \subseteq \sigma_1 Z_k \cup \sigma_2 Z_k \cup \cdots \cup \sigma_l Z_k.$$

综合以上结果得到

$$G = \sigma_1 Z_k \cup \sigma_2 Z_k \cup \cdots \cup \sigma_l Z_k.$$

又由于 $\sigma_i Z_k \cap \sigma_j Z_k = \varnothing (i \neq j)$,因此有

$$|\sigma_1 Z_k| + |\sigma_2 Z_k| + \cdots + |\sigma_l Z_k| = |G|.$$

方案6.换句话说，在一个置换群的作用下，方案3,4,5,6是彼此等价的. 原来的计数问题实际上是计数在一个置换群作用下的不同的等价类的个数. 不难看出共有6个等价类：{1}，{2}，{3,4,5,6}，{7,8,9,10}，{11,12}，{13,14,15,16}. 为了解决这种等价类的计数问题，我们需要另外一个重要的计数定理——Polya定理. 本节先引入置换群的有关概念和Burnside引理.

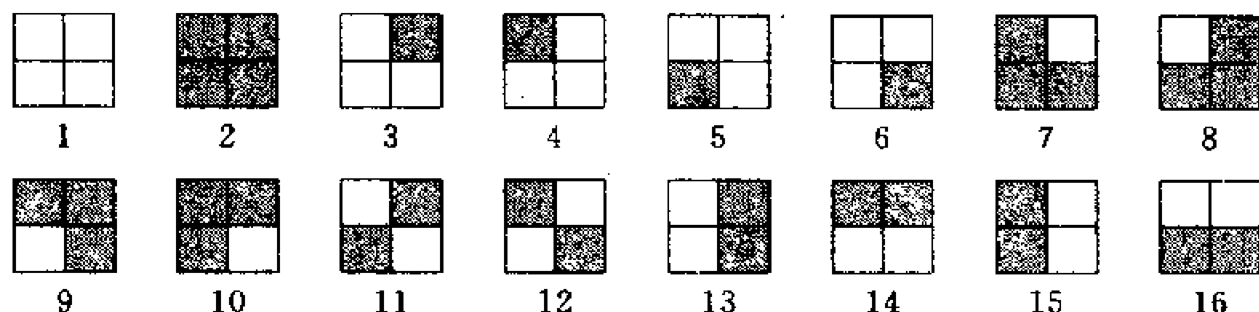


图 9.4

定义 9.2　设 $N=\{1,2,\cdots,n\}$，G 是 N 上的置换群. 对于任意的 $k\in N$，称置换的集合

$$Z_k=\{\sigma|\sigma\in G\wedge\sigma(k)=k\}$$

是 k 的**不变置换类**①.

例如 $G=\{(1),(12),(34),(12)(34)\}$ 是 S_4 的子群，则 $Z_1=Z_2=\{(1),(34)\}$，$Z_3=Z_4=\{(1),(12)\}$.

不验证明，$\forall k\in N$，Z_k 是 G 的子群.

定义 9.3　设 $N=\{1,2,\cdots,n\}$，G 是 N 上的置换群，R 是 N 上的等价关系且 $\forall x,y\in N$ 有

$$xRy\Leftrightarrow\exists\sigma(\sigma\in G\wedge\sigma(x)=y).$$

对于任意 $k\in N$，称 k 关于 R 的等价类是 k 的**轨道**，记作 E_k，即

$$E_k=\{l|l\in N\wedge kRl\}.$$

例如 $G=\{(1),(12),(34),(12)(34)\}$，则有

① k 的不变置换类也叫做 k 的稳定类

数了使得 j 保持不变的 G 中置换个数，即 $|Z_j|$. 由此得到

$$\sum_{k=1}^{g} c_1(\sigma_k) = \sum_{k=1}^{g}\sum_{j=1}^{n} s_{kj} = \sum_{j=1}^{n}\sum_{k=1}^{g} s_{kj} = \sum_{j=1}^{n}|Z_j|. \qquad ①$$

根据定理 9.6 有 $|Z_j| = |G|/|E_j|$，代入 ① 式得

$$\sum_{j=1}^{n}\frac{|G|}{|E_j|} = \sum_{k=1}^{g} c_1(\sigma_k). \qquad ②$$

假设 $i_1, i_2, \cdots, i_l$ 是同一轨道上的全体元素，则由等价类的性质得

$$E_{i_1} = E_{i_2} = \cdots = E_{i_l} \text{ 和 } |E_{i_l}| = l.$$

这说明

$$\frac{1}{|E_{i_1}|} + \frac{1}{|E_{i_2}|} + \cdots + \frac{1}{|E_{i_l}|} = 1.$$

将 ② 式左边所有的 $1/|E_j|\,(j = 1, 2, \cdots, n)$ 按轨道进行合并，每个轨道合并的结果都是 1，因此合并后的 ② 式就变成了

$$M \cdot |G| = \sum_{k=1}^{g} c_1(\sigma_k),$$

其中 M 是轨道个数，即

$$M = \frac{1}{|G|}\sum_{k=1}^{g} c_1(\sigma_k). \qquad \blacksquare$$

【例 9.13】 回顾 2×2 方格棋盘的涂色问题. 我们把因棋盘转动而引起涂色方案的转变看作是涂色方案集合上的置换群的作用. 设 $\overline{N}$ 是图 9.4 中的涂色方案的集合，$\overline{G}$ 是置换群，则

$$\overline{N} = \{1, 2, \cdots, 16\},$$
$$\overline{G} = \{\overline{\sigma}_1 = (1), \overline{\sigma}_2, \overline{\sigma}_3, \overline{\sigma}_4\},$$

其中 $\overline{\sigma}_1$ 代表棋盘不动，$\overline{\sigma}_2$ 代表棋盘逆时针转 90°，$\overline{\sigma}_3$ 代表棋盘逆时针转 180°，$\overline{\sigma}_4$ 代表棋盘逆时针转 270°. 将 $\overline{\sigma}_1, \overline{\sigma}_2, \overline{\sigma}_3$ 和 $\overline{\sigma}_4$ 的轮换表示式

$$\overline{\sigma}_1 = (1)(2)\cdots(16),$$

即

$$|Z_k| \cdot l = |Z_k| \cdot |E_k| = |G|. \qquad \blacksquare$$

例如 $G = S_3 = \{(1),(12),(13),(23),(123),(132)\}$,那么有 $|G| = 6$. 如果令 $k = 1$, 则 $E_1 = \{1,2,3\}$, $Z_1 = \{(1),(23)\}$, $|Z_1| \cdot |E_1| = 2 \times 3 = 6$.

Burnside 引理 设 $N = \{1,2,\cdots,n\}$,G 是 N 上的置换群. 令 $G = \{\sigma_1, \sigma_2, \cdots, \sigma_g\}$, $c_1(\sigma_k)$ 是 σ_k 的轮换表示式(见定理 3.16)中 1-轮换的个数. 又设 M 是不同的轨道个数,则有

$$M = \frac{1}{|G|}\sum_{k=1}^{g} c_1(\sigma_k).$$

证 对于 $k = 1,2,\cdots,g$,$c_1(\sigma_k)$ 表示在置换 σ_k 作用下保持不变的 N 中元素的个数,那么 $\sum\limits_{k=1}^{g} c_1(\sigma_k)$ 则表示在 G 中所有置换的作用下保持不变的 N 中元素的总数(包括重复计数). 如表 9.1 所示,其中的元素 s_{kj} 是 0 或 1($k = 1,2,\cdots,g$, $j = 1,2,\cdots,n$). 若 $\sigma_k(j) = j$,则 $s_{kj} = 1$,否则 $s_{kj} = 0$.

表 9.1

G 中元素 \ N 中元素	1	2	3	$\cdots$	n	$c_1(\sigma_k)$
$\sigma_1 = (1)$	s_{11}	s_{12}	s_{13}	$\cdots$	s_{1n}	$c_1(\sigma_1)$
σ_2	s_{21}	s_{22}	s_{23}	$\cdots$	s_{2n}	$c_1(\sigma_2)$
$\vdots$	$\cdots$					$\vdots$
σ_g	s_{g1}	s_{g2}	s_{g3}	$\cdots$	s_{gn}	$c_1(\sigma_g)$
$\lvert Z_j\rvert$	$\lvert Z_1\rvert$	$\lvert Z_2\rvert$	$\lvert Z_3\rvert$	$\cdots$	$\lvert Z_n\rvert$	$\sum\limits_{k=1}^{g} c_1(\sigma_k) = \sum\limits_{j=1}^{n} \lvert Z_j\rvert$

在表中 σ_k 所在的一行里,$\sum\limits_{j=1}^{n} s_{kj}$ 的值计数了在 σ_k 作用下保持不变的 N 中元素的个数,即 $c_1(\sigma_k)$. 而表的第 j 列的元素之和 $\sum\limits_{k=1}^{g} s_{kj}$ 又计

$$M = \frac{1}{24} \cdot 6! = 30.$$

§9.4 Polya 定理

Burnside 引理使用起来不太方便.如果有 n 个物体,用 m 种颜色涂色,我们先要给出 m^n 种涂色方案,然后分析这些方案在置换群作用下的结果.对于稍微大一些的 n 和 m 就是非常繁重的工作,有时候甚至是不可能完成的.Polya 定理是 Burnside 引理的推广.它们的区别在于:对于 Burnside 引理,置换群 $\overline{G}$ 是作用在 m^n 种涂色方案的集合上.而对于 Polya 定理,置换群 G 是作用在 n 个涂色的物体的集合上.显然后一个集合比前一个集合要小得多,群 G 比群 $\overline{G}$ 也要简单得多.

定理 9.7 (Polya 定理)设 $N = \{1,2,\cdots,n\}$,$G = \{\sigma_1,\sigma_2,\cdots,\sigma_g\}$ 是 N 上的置换群.用 m 种颜色对 N 中的元素进行涂色,则在 G 的作用下不同的涂色方案数是

$$M = \frac{1}{|G|}\sum_{k=1}^{g} m^{c(\sigma_k)},$$

其中 $c(\sigma_k)$ 是置换 σ_k 的轮换表示式中包括 1- 轮换在内的轮换个数.

证 设 $R = \{r_1,r_2,\cdots,r_m\}$ 是 m 种颜色的集合.对 N 中元素的任何一种涂色方案实际上就是一个从 N 到 R 的映射 f: $N \to R$,因此集合

$$R^N = \{f \mid f: N \to R\}$$

恰好代表所有涂色方案的集合.易见 $|R^N| = m^n$.

对于任意 $\sigma_k \in G$,σ_k: $N \to N$ 将诱导出一个 R^N 上的置换 τ_{σ_k}: $R^N \to R^N$,其中 $\tau_{\sigma_k}(f) = f\sigma_k$,$\forall f \in R^N$.不难验证 τ_{σ_k} 就是 σ_k 作用于 N 中元素所引起的涂色方案的置换.设

$$\overline{G} = \{\tau_{\sigma_k} \mid \sigma_k \in G\}$$

是 G 所诱导的 R^N 上的置换构成的集合,又令映射 φ: $G \to \overline{G}$,使得

$\bar{\sigma}_2 = (1)(2)(3\ 4\ 5\ 6)(7\ 8\ 9\ 10)(11\ 12)(13\ 14\ 15\ 16),$

$\bar{\sigma}_3 = (1)(2)(3\ 5)\ (4\ 6)(7\ 9)(8\ 10)(11)(12)(13\ 15)(14\ 16),$

$\bar{\sigma}_4 = (1)(2)(6\ 5\ 4\ 3)\ (10\ 9\ 8\ 7)(11\ 12)(16\ 15\ 14\ 13)$

代入 Burnside 引理得

$$M = \frac{1}{4}(16 + 2 + 4 + 2) = 6.$$

不同的涂色方案有 6 种，如图 9.5 所示.

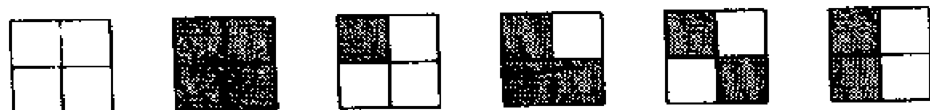


图 9.5

【例 9.14】 用 6 种颜色涂色一个立方体的六个面，如果要求每个面的颜色必须不同，且立方体可以在空间任意移动或转动，问有多少种不同的涂色方案?

解 先分析群 $\overline{G}$ 的结构，如图 9.6，$\overline{G}$ 中的置换可分成以下几类：

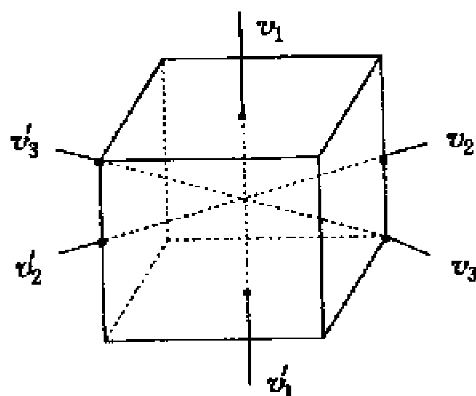


图 9.6

恒等置换 1 个

以过每一对平行平面的中心的直线(如 v_1v_1') 为轴，逆时针旋转 90°，180°，270° 有 3 个置换，那么三对平面共有 9 个置换.

以过每一对顶点的直线(如 v_3v_3') 为轴转动 120° 或 240° 有 2 个置换，那么四对顶点共有 8 个置换.

以过每一对棱的中心的直线(如 v_2v_2') 为轴转动 180° 有 1 个置换，那么六对棱共有 6 个置换.

综上所述，群 $\overline{G}$ 中有 24 个置换，其中除了恒等置换以外，在别的置换的作用下涂色方案都要发生变化，而在恒等置换作用下，不变的方案有 6! 个. 根据 Burnside 引理，不同的涂色方案数是

把这个等式代入 Burnside 引理得

$$M = \frac{1}{|G|}\sum_{k=1}^{g} c_1(\tau_{\sigma_k}) = \frac{1}{|G|}\sum_{k=1}^{g} m^{c(\sigma_k)}. \quad \blacksquare$$

【例 9.15】 让我们重新考虑 2×2 方格棋盘的涂两色问题. 根据题意有 $N = \{1,2,3,4\}, G = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$,其中

$$\sigma_1 = (1)(2)(3)(4), \qquad \sigma_2 = (1\ 2\ 3\ 4),$$
$$\sigma_3 = (13)(24), \qquad \sigma_4 = (4\ 3\ 2\ 1).$$

将 $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ 代入定理 9.7 得

$$M = \frac{1}{4}(2^4 + 2^1 + 2^2 + 2^1) = \frac{1}{4}(16 + 2 + 4 + 2) = 6.$$

【例 9.16】 如图 9.7,用三种颜色涂色装有 5 颗珠子的手镯. 如果只考虑手镯的旋转,问有多少种涂色方案?

解 $m = 3$, $N = \{1,2,3,4,5\}$, $G = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5\}$,其中

$\sigma_1 = (1)(2)(3)(4)(5)$ 不动,

$\sigma_2 = (1\ 2\ 3\ 4\ 5)$ 逆时针转 72°,

$\sigma_3 = (1\ 3\ 5\ 2\ 4)$ 逆时针转 144°,

$\sigma_4 = (1\ 4\ 2\ 5\ 3)$ 逆时针转 216°,

$\sigma_5 = (1\ 5\ 4\ 3\ 2)$ 逆时针转 288°.

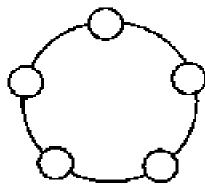


图 9.7

代入定理 9.7 得

$$M = \frac{1}{5}(3^5 + 3^1 + 3^1 + 3^1 + 3^1) = 51.$$

【例 9.17】 证明 Fermat 小定理:若 p 为素数,则 p 整除 $n^p - n$.

证 如例 9.16,考虑用 n 种颜色涂色装有 p 颗珠子的手镯. 若手镯只能旋转,则 $|G| = p$. 因为 p 是素数,G 是循环群. 除了恒等置换以外,G 中的其它置换都是只含有一个轮换的置换. 由定理 9.7 得到不同的手镯数是

$$M = \frac{1}{p}(n^p + \underbrace{n^1 + n^1 + \cdots + n^1}_{p-1\text{个}}),$$

$$\varphi(\sigma_k) = \tau_{\sigma_k^{-1}},\ \forall \sigma_k \in G,$$

则 φ 是 G 到 $\overline{G}$ 的同构映射. 先证 φ 是同态. 对任意 σ_k, $\sigma_l \in G$, 若 $\sigma_k\sigma_l = \sigma_t$, 则 $\forall f \in R^N$ 有

$$\begin{aligned}\varphi(\sigma_k\sigma_l)(f) &= \varphi(\sigma_t)(f) = \tau_{\sigma_t^{-1}}(f) = f\sigma_t^{-1} = f(\sigma_k\sigma_l)^{-1} \\ &= f\sigma_l^{-1}\sigma_k^{-1},\end{aligned}$$

$$\varphi(\sigma_k)\varphi(\sigma_l)(f) = \tau_{\sigma_k^{-1}}(\tau_{\sigma_l^{-1}}(f)) = \tau_{\sigma_k^{-1}}(f\sigma_l^{-1}) = f\sigma_l^{-1}\sigma_k^{-1},$$

即

$$\varphi(\sigma_k\sigma_l) = \varphi(\sigma_k)\varphi(\sigma_l),$$

φ 是 G 到 $\overline{G}$ 的同态.

再证明 φ 是单射. 设 $\varphi(\sigma_k) = \varphi(\sigma_l)$, 即 $\forall f \in R^N$ 有 $f\sigma_k^{-1} = f\sigma_l^{-1}$, 必有 $\sigma_k^{-1} = \sigma_l^{-1}$. 若不然, 存在 $i \in \{1,2,\cdots,n\}$ 使得 $\sigma_k^{-1}(i) \neq \sigma_l^{-1}(i)$. 构造 $f: N \to R$, 使得 $f(\sigma_k^{-1}(i)) \neq f(\sigma_l^{-1}(i))$, 则与 $f\sigma_k^{-1} = f\sigma_l^{-1}$ 矛盾, 从而推出 $\sigma_k = \sigma_l$.

最后证明 φ 是满射. $\forall \tau_{\sigma_t} \in \overline{G}$, $\exists\ \sigma_t^{-1} \in G$, 使得

$$\varphi(\sigma_t^{-1}) = \tau_{(\sigma_t^{-1})^{-1}} = \tau_{\sigma_t}.$$

综上所述, φ 是 G 到 $\overline{G}$ 的同构, 因此有 $|\overline{G}| = |G|$. 称 $\overline{G}$ 是 G 所诱导的涂色方案集合上的置换群.

设 σ_k 是 G 中的置换, 且它的轮换表示式是

$$\sigma_k = \underbrace{(\cdot\cdot\ \cdots\ \cdot)(\cdot\cdot\ \cdots\ \cdot)\cdots(\cdot\cdot\ \cdots\ \cdot)}_{c(\sigma_k)\text{个轮换}}.$$

如果属于同一个轮换的数字被涂上同样的颜色, 这样的涂色方案在 τ_{σ_k} 的作用下是不变的, 所以它属于 τ_{σ_k} 的不变元素. 另一方面, 如果有一种涂色方案使得 σ_k 的某个轮换中出现了不同的颜色, 则在该轮换中必有两个相邻的数字具有不同的颜色. 于是在 τ_{σ_k} 的作用下必得到不同的涂色方案. 这就证明了在 τ_{σ_k} 作用下不变的涂色方案数 $c_1(\tau_{\sigma_k})$ 应该等于对 σ_k 的同一轮换涂同色的方案数, 即

$$c_1(\tau_{\sigma_k}) = m^{c(\sigma_k)},$$

定理 9.8 设 $D=\{1,2,\cdots,n\}$，$R=\{1,2,\cdots,m\}$，R 对 D 的所有可能的着色方案的集合为 S，则 S 的清单是

$$W=[w(1)+w(2)+\cdots+w(m)]^n.$$

证 上述乘积展开式的每一项由 n 个因子组成，它们的一般形式是

$$w(i_1)w(i_2)\cdots w(i_n),\ i_1,i_2,\cdots,i_n\in\{1,2,\cdots,m\}.$$

这正是着色方案 f：$1\mapsto i_1$，$2\mapsto i_2$，$\cdots$，$n\mapsto i_n$ 的权. 所有的着色方案是 m^n 种，正好对应了展开式的 m^n 个项，所以清单

$$W=\sum_{\substack{1\leqslant i_j\leqslant m\\ j=1,2,\cdots,n}} w(i_1)w(i_2)\cdots w(i_n)=[w(1)+\cdots+w(m)]^n. \qquad ∎$$

定理 9.9 设 $D=\{1,2,\cdots,n\}$，$R=\{1,2,\cdots,m\}$. 将 D 划分成 k 个不交的子集 $D_1,D_2,\cdots,D_k$，然后用 R 中的颜色对 D 中的数字着色. 如果要求在同一子集中的数字必须着同色，且将所有这种着色方案构成的集合记作 S，则 S 的清单是

$$\begin{aligned}W=&[w(1)^{|D_1|}+w(2)^{|D_1|}+\cdots+w(m)^{|D_1|}]\\&\cdot[w(1)^{|D_2|}+w(2)^{|D_2|}+\cdots+w(m)^{|D_2|}]\\&\cdot\cdots\\&\cdot[w(1)^{|D_k|}+w(2)^{|D_k|}+\cdots+w(m)^{|D_k|}].\end{aligned}$$

证 上述乘积展开式中的项都是如下的形式：

$$w(i_1)^{|D_1|}w(i_2)^{|D_2|}\cdot\cdots\cdot w(i_k)^{|D_k|},$$

它是对 D_1 中的数字着 i_1 色，对 D_2 中的数字着 i_2 色，$\cdots$，对 D_k 中的数字着 i_k 色的着色方案的权. 因为 $i_1,i_2,\cdots,i_k$ 遍取了所有可能的颜色，共有 m^k 种方案，对应了乘积展开式中的 m^k 个项，所以

$$\sum w(i_1)^{|D_1|}w(i_2)^{|D_2|}\cdots w(i_k)^{|D_k|}$$

就是 S 的清单. ∎

【例 9.19】 投掷五个骰子 d_1,d_2,d_3,d_4,d_5，有多少种布局使得 d_1,d_2,d_3 的点数相同，d_4,d_5 的点数相同，并且总和为 19.

化简上式得

$$M = \frac{1}{p}[n^p + (p-1)n] = \frac{1}{p}(n^p - n + pn).$$

因为 M 是整数，且 p 整除 pn，所以 p 一定整除 $n^p - n$. ∎

下面我们考虑 Polya 定理的一般形式 —— 带权的 Polya 定理. 当我们需要计算带有某些限制条件的着色方案数，或者需要知道具体的着色方案的种类，那么就要用到带权的 Polya 定理. 先给出有关权的概念和定理.

定义 9.4　设 $D = \{1,2,\cdots,n\}$ 是 n 个数字的集合，$R = \{c_1, c_2, \cdots, c_m\}$ 是 m 种颜色的集合. 对于任何一种颜色 c_r，$w(c_r)$ 是该颜色的权. 设 $f: D \to R$ 是一种着色方案，则称该方案所有被着颜色的权之积为该**方案的权**，记作 $w(f)$，即

$$w(f) = \prod_{i=1}^{n} w(f(i)).$$

【例 9.18】　设 $D = \{1,2,3,4\}$，$R = \{$红，蓝$\}$，给定颜色的权为 $w($红$) = 2$，$w($蓝$) = 3$，则着色方案 f：$1 \mapsto$ 红，$2 \mapsto$ 蓝，$3 \mapsto$ 红，$4 \mapsto$ 红的权

$$w(f) = w(\text{红})w(\text{蓝})w(\text{红})w(\text{红}) = 24.$$

如果令 $w($红$) =$ 红，$w($蓝$) =$ 蓝，则 f 的权

$$w(f) = \text{红蓝红红}.$$

其实这就是方案 f 本身. 如果令 $w($红$) = w($蓝$) = 1$，则 $w(f) = 1$.

定义 9.5　设 S 是着色方案的集合，称 S 中所有着色方案的权之和为 S 的**清单**，记作 W，即

$$W = \sum_{f \in S} w(f).$$

在例 9.18 中，如果令 $w($红$) =$ 红，$w($蓝$) =$ 蓝，则任一着色方案的权就是该方案本身，所以清单恰好以和的形式给出了所有的着色方案. 如果令 $w($红$) = w($蓝$) = 1$，则任何一种着色方案的权都是 1，这时清单就是着色方案的总数.

边得

$$\left[\frac{w(f_1)}{|E_{f_1}|}+\frac{w(f_2)}{|E_{f_2}|}+\cdots\quad\right].$$

在同一轨道上任何方案的权就等于轨道的权. 我们把上式中在同一轨道上的所有的项相加,就得到这个轨道的权,所以整个式子正好是所有轨道的权之和. ∎

在定理 9.10 中如果规定所有颜色的权都是 1 时,那么着色方案的权也是 1,从而任何轨道的权也是 1. 这时等式左边就计数了不同的轨道个数,而右边的每一项 $\overline{w}(\overline{\sigma}_k)$ 则计数了在 $\overline{\sigma}_k$ 作用下保持不变的着色方案个数. 这时定理 9.10 就变成了 Burnside 引理,所以这个定理也叫做带权的 Burnside 定理.

定理 9.11　设 $D=\{1,2,\cdots,n\}$ 是物体的集合,$R=\{1,2,\cdots,m\}$ 是颜色的集合,$G=\{\sigma_1,\sigma_2,\cdots,\sigma_g\}$ 是 D 上的置换群. 对于任意的着色方案 $f\in R^D$,$w(f)$ 是 f 的权,则所有不同的着色方案轨道的权之和是:

$$\begin{aligned}&\frac{1}{|G|}\left[w_1^{c_1(\sigma_1)}w_2^{c_2(\sigma_1)}\cdots w_n^{c_n(\sigma_1)}\right.\\&+w_1^{c_1(\sigma_2)}w_2^{c_2(\sigma_2)}\cdots w_n^{c_n(\sigma_2)}\\&+\cdots\cdots\cdots\cdots\cdots\cdots\\&\left.+w_1^{c_1(\sigma_g)}w_2^{c_2(\sigma_g)}\cdots w_n^{c_n(\sigma_g)}\right],\end{aligned}$$

其中

$$\begin{aligned}w_1&=w(1)+w(2)+\cdots+w(m),\\w_2&=w(1)^2+w(2)^2+\cdots+w(m)^2,\\&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\w_n&=w(1)^n+w(2)^n+\cdots+w(m)^n.\end{aligned}$$

证　由定理 9.10 和 $|G|=|\overline{G}|$ 知道所有不同着色方案轨道的权之和是

解 令$D=\{d_1,d_2,d_3,d_4,d_5\}$. 将$D$划分成两个子集$D_1$和$D_2$，其中$D_1=\{d_1,d_2,d_3\}$，$D_2=\{d_4,d_5\}$. 令颜色的集合$R=\{1,2,3,4,5,6\}$，并且规定对任意的颜色$i$，$i$的权$w(i)=x^i$. 不难看出任何一种布局就是一种着色方案，它的权是x的幂，而幂指数就是该布局的总点数. 由定理9.9得

$$w=[(x^1)^3+(x^2)^3+\cdots+(x^6)^3]\cdot[(x^1)^2+(x^2)^2+\cdots+(x^6)^2].$$

上式中x^{19}的系数是2，它是由

$$(x^3)^3\cdot(x^5)^2+(x^5)^3\cdot(x^2)^2$$

而得到的，这就给出了两种可能的布局，即

d_1,d_2,d_3的点数是3，d_4和d_5的点数是5；

d_1,d_2,d_3的点数是5，d_4和d_5的点数是2.

下面给出带权的Burnside定理和Polya定理.

定理9.10 设D是物体的集合，R是颜色的集合，S是着色方案的集合. $\overline{G}=\{\overline{\sigma}_1,\overline{\sigma}_2,\cdots,\overline{\sigma}_g\}$是$S$上的置换群. 对于任意的着色方案$f\in S$，$f$的权记作$w(f)$，且满足下面的性质：

$$w(f)=w(\overline{\sigma}_k(f)),\quad k=1,2,\cdots,g,$$

即在同一轨道上的着色方案的权都相等. 设关于$\overline{G}$的轨道是$E_1,E_2,\cdots,E_l$，定义轨道的权为轨道中着色方案的公共权，即

$$w(E_i)=\underset{f\in E_i}{w(f)},\ i=1,2,\cdots,l.$$

对于任意的$\overline{\sigma}_k\in\overline{G}$，令$\overline{w}(\overline{\sigma}_k)$是在$\overline{\sigma}_k$作用下保持不变的那些着色方案的权之和，则

$$\sum_{i=1}^{l}w(E_i)=\frac{1}{|\overline{G}|}\sum_{k=1}^{g}\overline{w}(\overline{\sigma}_k).$$

证 等式右边的每一项$\overline{w}(\overline{\sigma}_k)$计数了在$\overline{\sigma}_k$作用下保持不变的着色方案的权之和. 对于方案$f$来说，$w(f)$在右边出现的次数就是$\overline{G}$中使得$f$保持不变的置换个数$|Z_f|$，将$|Z_f|=|\overline{G}|/|E_f|$代入右

$$\frac{1}{|G|}[m^{c(\sigma_1)}+m^{c(\sigma_2)}+\cdots+m^{c(\sigma_g)}]=\frac{1}{|G|}\sum_{k=1}^{g}m^{c(\sigma_k)},$$

从而得到了定理 9.7(Polya 定理).

【例9.20】 如图 9.8 所示，用四颗珠子穿项链，其中两颗蓝色，一颗红色，一颗黄色，问可以有多少种不同的方案？

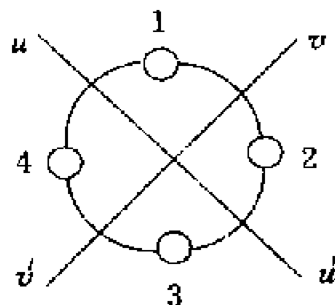


图 9.8

解 令 $D=\{1,2,3,4\}$，$R=\{$蓝，红，黄$\}$，且规定

$$w(\text{蓝})=b,\ w(\text{红})=r,\ w(\text{黄})=y.$$

作用于 D 上的置换群 G 是

G:	$\sigma_1=(1)(2)(3)(4)$	不动
	$\sigma_2=(1\ 2\ 3\ 4)$	逆时针旋转 90°
	$\sigma_3=(13)(24)$	逆时针旋转 180°
	$\sigma_4=(4\ 3\ 2\ 1)$	逆时针旋转 270°
	$\sigma_5=(1)(3)(24)$	以 1 和 3 为轴翻转 180°
	$\sigma_6=(2)(4)(13)$	以 2 和 4 为轴翻转 180°
	$\sigma_7=(12)(34)$	以 vv' 为轴翻转 180°
	$\sigma_8=(14)(23)$	以 uu' 为轴翻转 180°

且

$$w_1=b+r+y,\qquad w_2=b^2+r^2+y^2,$$

$$w_3=b^3+r^3+y^3,\quad w_4=b^4+r^4+y^4.$$

代入定理 9.11 得

$$W=\frac{1}{8}[w_1^4+w_4^1+w_2^2+w_4^1+w_1^2w_2+w_1^2w_2+w_2^2+w_2^2]$$

$$=\frac{1}{8}[w_1^4+2w_4+2w_1^2w_2+3w_2^2]$$

$$=\frac{1}{8}[(b+r+y)^4+2(b^4+r^4+y^4)$$
$$+2(b+r+y)^2(b^2+r^2+y^2)+3(b^2+r^2+y^2)^2]$$

$$\frac{1}{|G|}[\overline{w}(\overline{\sigma}_1) + \overline{w}(\overline{\sigma}_2) + \cdots + \overline{w}(\overline{\sigma}_g)], \qquad ①$$

其中 $\overline{w}(\overline{\sigma}_k)$ 是在 $\overline{\sigma}_k$ 作用下保持不变的着色方案的权之和. $\forall k \in \{1, 2, \cdots, g\}$, 设和 $\overline{\sigma}_k$ 相对应的置换 σ_k 的轮换表示式中有 t 个轮换,即

$$\sigma_k = \tau_1\tau_2\cdots\tau_t.$$

由定理 9.9,在 $\overline{\sigma}_k$ 作用下保持不变的着色方案的权之和 $\overline{w}(\overline{\sigma}_k)$ 等于

$$\begin{aligned}&[w(1)^{|\tau_1|} + w(2)^{|\tau_1|} + \cdots + w(m)^{|\tau_1|}]\\ &\cdot [w(1)^{|\tau_2|} + w(2)^{|\tau_2|} + \cdots + w(m)^{|\tau_2|}]\\ &\cdot \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &\cdot [w(1)^{|\tau_t|} + w(2)^{|\tau_t|} + \cdots + w(m)^{|\tau_t|}],\end{aligned}$$

其中 $|\tau_j|$ 表示 τ_j 中的元素个数, $j = 1, 2, \cdots, t$. 以上乘积中的每一个因式具有下面的形式

$$w_s = w(1)^s + w(2)^s + \cdots + w(m)^s,$$

而 w_s 出现的次数正好是 σ_k 的轮换表示式中阶为 s 的轮换个数,即 $c_s(\sigma_k)$,所以有

$$\overline{w}(\overline{\sigma}_k) = w_1^{c_1(\sigma_k)} w_2^{c_2(\sigma_k)} \cdots w_n^{c_n(\sigma_k)}.$$

把所有的 $\overline{w}(\overline{\sigma}_k)(k = 1, 2, \cdots, g)$ 都表成上述形式并代入 ① 式,定理得证. ∎

定理 9.11 称为带权的 Polya 定理. 如果令所有的颜色的权都是 1,则在定理中有

$$w_1 = w_2 = \cdots = w_n = m,$$

那么定理的结果就变成

$$\frac{1}{|G|}[m^{c_1(\sigma_1)} m^{c_2(\sigma_1)} \cdots m^{c_n(\sigma_1)} + m^{c_1(\sigma_2)} m^{c_2(\sigma_2)} \cdots m^{c_n(\sigma_2)}$$
$$+ \cdots + m^{c_1(\sigma_g)} m^{c_2(\sigma_g)} \cdots m^{c_n(\sigma_g)}].$$

因为 $c_1(\sigma_k) + c_2(\sigma_k) + \cdots + c_n(\sigma_k)$ 就是 σ_k 中轮换的个数 $c(\sigma_k)$, $k = 1, 2, \cdots, g$. 化简上式得

习 题 九

1. 在 1 和 10000 之间(包括 1 和 10000 在内)不能被 4,5 和 6 整除的数有多少个?

2. 在 1 和 10000 之间(包括 1 和 10000 在内)既不是某个整数的平方,也不是某个整数的立方的数有多少个?

3. 在 1 和 500 之间(包括 1 和 500 在内)不能被 7 整除但能被 3 或 5 整除的数有多少个?

4. 确定 $S = \{\infty \cdot a,\ 3 \cdot b,\ 5 \cdot c,\ 7 \cdot d\}$ 的 10- 组合数.

5. (1) 确定方程 $x_1 + x_2 + x_3 = 14$ 的不超过 8 的非负整数解的个数;

(2) 确定方程 $x_1 + x_2 + x_3 = 14$ 的不超过 8 的正整数解的个数.

6. 有 7 本书放在书架上,先把书拿下来然后重新放回书架,求满足以下条件的放法数:

(1) 没有一本书在原来的位置上;

(2) 至少有一本书在原来的位置上;

(3) 至少有两本书在原来的位置上.

7. 求集合$\{1,2,\cdots,n\}$的排列数,使得在排列中正好有 k 个整数在它们的自然位置上(所谓自然位置就是整数 i 排在第 i 位).

8. 定义 $D_0 = 1$,用组合分析的方法证明

$$n! = \binom{n}{0}D_n + \binom{n}{1}D_{n-1} + \binom{n}{2}D_{n-2} + \cdots + \binom{n}{n}D_0.$$

9. 证明 D_n 为偶数当且仅当 n 为奇数.

10. 求多重集 $S = \{3 \cdot a,\ 4 \cdot b,\ 2 \cdot c\}$ 的排列数,使得在这些排列中同类字母的全体不能相邻(例如不允许 *abbbbccaa*,但允许 *aabbbacbc*).

11. 证明 $Q_n = D_n + D_{n-1}$.

12. 从一个 4×4 的棋盘中选取不在同一行也不在同一列上的两个方格,问有多少种方法?

13. 证明棋盘多项式的性质:

(1) $R(C) = xR(C_i) + R(C_l)$;

(2) $R(C) = R(C_1) \cdot (RC_2)$,其中 C_1 和 C_2 不存在公共的行和列.

$$=b^4+r^4+y^4+b^3r+b^3y+br^3+r^3y+by^3+ry^3$$
$$+2b^2r^2+2b^2y^2+2r^2y^2+2b^2ry+2br^2y+2bry^2.$$

上式中 b^2ry 项的系数是 2,因此有两种方案.图 9.9 给出了这两种方案的项链.

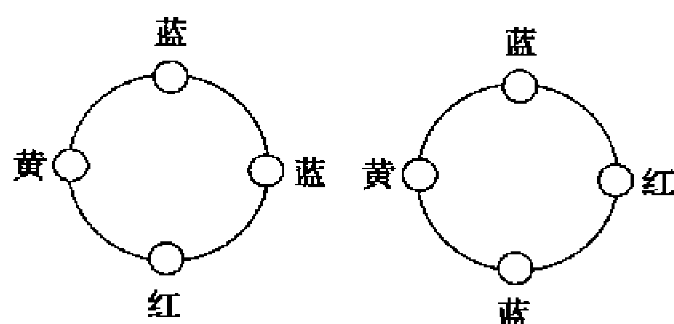


图 9.9

【例 9.21】 证明 3 个顶点的不同构的无向图有 4 个.

证 设 $D=\{1,2,3\}$ 是一个正三角形的边集,$R=\{$黑,白$\}$ 是颜色的集合,且 w(黑) $=b$,w(白) $=w$,如果一条边着黑色,则这条边在图中;如果着白色,就从图中去掉这条边.因此不同构的无向图个数恰好等于在 $G=S_3$ 作用下的不同的着色方案个数.由于

$$G=\{(1)(2)(3),(1)(23),(2)(13),(3)(12),(123),(132)\},$$

代入 Ploya 定理,所得的清单是

$$\frac{1}{6}(b+w)^3+3(b+w)(b^2+w^2)+2(b^3+w^3)]$$
$$=b^3+w^3+b^2w+bw^2.$$

图 9.10 给出了相应的 4 种着色方案.

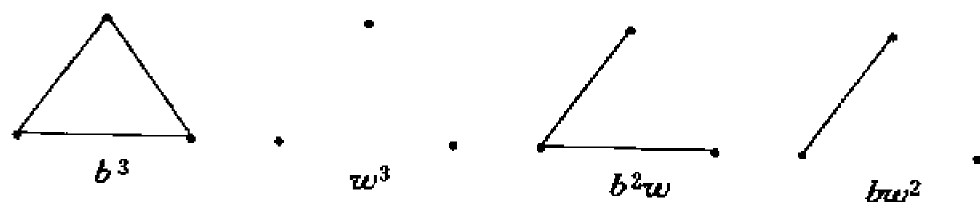


图 9.10

处颜色涂色 N 中数字的不同的涂色方案应该有多少种？

(2) 试用方程非负整数解的组合计数模型重新求解这一问题，并证明两种求解方法的结果是一样的.

27. 有一个正八面体，每个面都是正三角形，用两种颜色给八个面着色，如果八面体可以在空间任意转动，问有多少种方案？

28. (1) 证明给一个立方体的八个顶点着黑白两色的不同方案数是 23；

(2) 证明用 m 种颜色给立方体的顶点着色的不同方案数是

$$\frac{1}{24}(m^8 + 17m^4 + 6m^2);$$

(3) 证明如果 n 是正整数，则 24 可以整除 $n^8 + 17n^4 + 6n^2$.

29. 如图 9.11，T 是一棵七个结点的树，我们用黑白两色对 T 的结点着色. 如果交换 T 的某个左子树与右子树以后，一种着色方案 f_1 就变成另一种着色方案 f_2，则认为 f_1 和 f_2 是同样的着色方案. 问不同的着色方案有多少种？

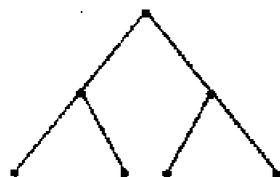


图 9.11

30. 一个立方体可以在空间转动，用黑白两色对它的六个面着色.

(1) 若要求三个面着黑色，三个面着白色，那么不同的方案有多少种？

(2) 若要求四个面着黑色，二个面着白色，那么不同的方案有多少种？

(3) 如果不加任何限制，有多少种着色方案？

(4) 证明用 m 种颜色给立方体的面着色，不加任何限制的着色方案数是

$$\frac{1}{24}(m^6 + 3m^4 + 12m^3 + 8m^2).$$

31. 用 m 种颜色对一根 8 尺长的均匀木棍着色，每尺着一种颜色，如果相邻的两尺不能着同色，问有多少种着色方案？

14. 计算 $h \begin{array}{lll} \square & & \\ \square & \square & \\ \square & \square & \square \end{array}$

15. 有 4 个人，分别记作 x_1, x_2, x_3 和 x_4. 有 5 项工作，分别记作 y_1, y_2, y_3, y_4 和 y_5. 已知 x_1 可以承担 y_1 或 y_3，x_2 可以承担 y_2 或 y_5，x_3 可以承担 y_2 或 y_4，x_4 可以承担 y_3. 要使每个人承担一项工作且每个人的工作都不相同，问有多少种分配方案？

16. 排列字母 A, B, C, D, E, F, G, H，如果要求既不出现 BEG，也不出现 CAD，问有多少种不同的方式？

17. 把 15 个人分到 3 个不同的房间，每个房间至少一个人，问有多少种分法？

18. (1) 有 1 和 1000000 之间(包括 1 的 1000000 在内)有多少个整数包含了数字 1,2,3 和 4?

(2) 在 1 和 1000000 之间(包括 1 和 1000000 在内)有多少个整数只由数字 1,2,3 或 4 构成?

19. 写出 S_4 的所有共轭类的轮换指数，并列出相应于每一种轮换指数的共轭类中的置换.

20. 设 $\sigma \in S_n$ 的轮换指数为 $1^{c_1}2^{c_2}\cdots n^{c_n}$，证明 σ 的奇偶性与 $c_2 + c_4 + c_6 + \cdots$ 一样.

21. 证明在轮换指数为 $1^{c_1}2^{c_2}\cdots n^{c_n}$ 的共轭类中有

$$N = \frac{n!}{c_1!c_2!\cdots c_n!\ 1^{c_1}2^{c_2}\cdots n^{c_n}}$$

个置换.

22. 证明 $\sum \frac{1}{c_1!c_2!\cdots c_n!\ 1^{c_1}2^{c_2}\cdots n^{c_n}} = 1$，其中求和是对方程 $c_1 + 2c_2 + \cdots + nc_n = n$ 的一切非负整数解来求.

23. 写出 S_4 的所有不变置换类.

24. 设 $N = \{1, 2, \cdots, n\}$，G 是 N 上的置换群，对于任意 $k \in N$，证明 k 的不变置换类 Z_k 是 G 的子群.

25. 设 $N = \{1, 2, \cdots, n\}$，G 是 N 上的置换群，如果 $G = \{(1)\}$，那么用 m 种颜色涂色 N 中数字的不同的涂色方案应有多少种？

26. (1) 设 $N = \{1, 2, \cdots, n\}$，G 是 N 上的置换群，如果 $G = \{S_n\}$，那么用 m

每行和每列中每个数字恰好出现一次，则称这个矩阵为一个**拉丁方**，n 称为该拉丁方的**阶**.

【例 10.2】 下面分别是 2 阶，3 阶和 4 阶的拉丁方：

$$\begin{bmatrix}1 & 2\\2 & 1\end{bmatrix}\quad\begin{bmatrix}1 & 2 & 3\\2 & 3 & 1\\3 & 1 & 2\end{bmatrix}\quad\begin{bmatrix}1 & 2 & 3 & 4\\4 & 3 & 2 & 1\\2 & 1 & 4 & 3\\3 & 4 & 1 & 2\end{bmatrix}.$$

对于任意给定的 n，可以利用下述排列

$$\begin{array}{lcccccccc}
\text{第 1 行} & 1 & 2 & 3 & \cdots & & & n-1 & n\\
\text{第 2 行} & n & 1 & 2 & \cdots & & & n-2 & n-1\\
\cdots & & & & & & & & \\
\text{第 } i \text{ 行} & n-i+2 & n-i+3 & \cdots & n & 1 & \cdots & n-i & n-i+1\\
\cdots & & & & & & & & \\
\text{第 } n \text{ 行} & 2 & 3 & 4 & \cdots & & & n & 1
\end{array}$$

构造一个 n 阶拉丁方. 按照这种方法，第 j 列的数字依次为 $j,j-1,\cdots,1,n,n-1,,\cdots,j+1$. 不难看出在每一行和每一列，$\{1,2,\cdots,n\}$ 中的任何数字恰好出现一次. 下面的 7 阶拉丁方

$$\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\7 & 1 & 2 & 3 & 4 & 5 & 6\\6 & 7 & 1 & 2 & 3 & 4 & 5\\5 & 6 & 7 & 1 & 2 & 3 & 4\\4 & 5 & 6 & 7 & 1 & 2 & 3\\3 & 4 & 5 & 6 & 7 & 1 & 2\\2 & 3 & 4 & 5 & 6 & 7 & 1\end{bmatrix}$$

就是按照这种方法构造出来的.

定义 10.2 设 $A=(a_{ij}),B=(b_{ij})$ 是两个 n 阶拉丁方，如果 n^2 个有序对 $\langle a_{ij},b_{ij}\rangle,i,j\in\{1,2,\cdots,n\}$，都是彼此不相等的，则称 A 与 B 是**正交**的.

第十章　组合设计与编码

组合设计也叫做块设计或区组设计，主要是研究实验安排. 请看下面的例子.

【例 10.1】 在试制某产品的过程中需要填加一种材料，填加的比例可能是 10%—13%，如果市场上的材料有 4 种，分别记作 1,2,3 和 4. 为了比较不同的材料及不同的填加比例对产品性能的影响需要做 16 个样品. 如果一次实验可以同时完成 4 个样品，那么可以有多种不同的实验方案. 图 10.1 就给出了两种不同的实验方案.

次 \ 比例	10	11	12	13
第一次	1	1	1	1
第二次	2	2	2	2
第三次	3	3	3	3
第四次	4	4	4	4

方案 1

次 \ 比例	10	11	12	13
第一次	1	2	3	4
第二次	2	3	4	1
第三次	3	4	1	2
第四次	4	1	2	3

方案 2

图　10.1

显然方案 2 比方案 1 好. 因为每次实验不可能处在完全相同的条件下，方案 2 在最大的程度上减少了因条件的差异对结果的影响.

通常称图 10.1 中的表为**区组设计**，其中的元素（例如 1,2,3,4）称作点，设计中的每个列称作区组或块. 设所有点的集合为 P，那么每个块 B_i 都是 P 的子集. 本章先讨论拉丁方（*latin Square*）—— 一种重要的区组设计，然后讨论 t- 设计，最后介绍编码理论以及它们和区组设计的关系.

§10.1　拉丁方

定义 10.1　由数字 1,2…,n 构成一个 $n\times n$ 的矩阵，若在它的

$$\begin{bmatrix}5&4&3&2&1\\4&3&2&1&5\\3&2&1&5&4\\2&1&5&4&3\\1&5&4&3&2\end{bmatrix}\qquad\begin{bmatrix}5&3&1&4&2\\4&2&5&3&1\\3&1&4&2&5\\2&5&3&1&4\\1&4&2&5&3\end{bmatrix}$$

肥料 A　　　　肥料 B

$$A,B\to\begin{bmatrix}\langle 5,5\rangle&\langle 4,3\rangle&\langle 3,1\rangle&\langle 2,4\rangle&\langle 1,2\rangle\\\langle 4,4\rangle&\langle 3,2\rangle&\langle 2,5\rangle&\langle 1,3\rangle&\langle 5,1\rangle\\\langle 3,3\rangle&\langle 2,1\rangle&\langle 1,4\rangle&\langle 5,2\rangle&\langle 4,5\rangle\\\langle 2,2\rangle&\langle 1,5\rangle&\langle 5,3\rangle&\langle 4,1\rangle&\langle 3,4\rangle\\\langle 1,1\rangle&\langle 5,4\rangle&\langle 4,2\rangle&\langle 3,5\rangle&\langle 2,3\rangle\end{bmatrix}$$

图　10.2

定义 10.3　设 F 为有限域(见 §4.1),对任意 $a,b\in F$,称有序对 $\langle a,b\rangle$ 是**点**.对于任意 $c,d,e\in F$,c,d 不全为 0,称集合

$$S=\{\langle x,y\rangle\,|\,x,y\in F\wedge cx+dy+e=0\}$$

为**线**或 F 所确定的线.线 S 可以简记为 $cx+dy+e=0$.

【例 10.5】　设 $F=\{0,1\}$,则 $\langle 0,0\rangle,\langle 0,1\rangle,\langle 1,0\rangle,\langle 1,1\rangle$ 是 F 上的点,而

$$x=0,y=0,x=1,y=1,$$
$$x+y=0,x+y=1$$

是 F 上的线.F 上所有的点和线如图 10.3 所示.

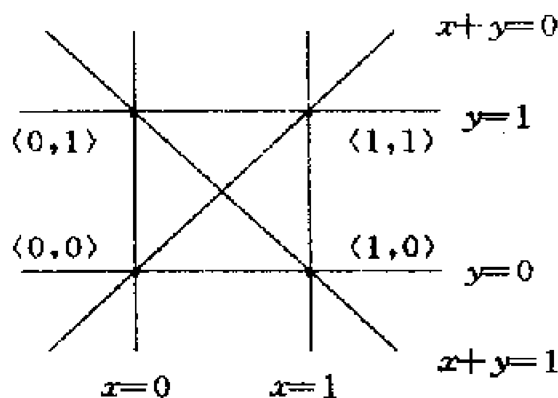


图　10.3

设 F 为有限域,$cx+dy+e=0$ 是 F 上的一条线,则 c,d 不全为 0.若 $d\neq 0$,则有

$$d^{-1}cx+y+d^{-1}e=0.$$

即

$$y=-d^{-1}cx-d^{-1}e.$$

若 $d=0$,则 $c\neq 0$,原方程化为 $cx+e=0$,则

【例 10.3】 设 A,B,C 是三个 4 阶拉丁方，其中

$$A=\begin{bmatrix}1&2&3&4\\2&3&4&1\\3&4&1&2\\4&1&2&3\end{bmatrix},\ B=\begin{bmatrix}4&3&2&1\\3&4&1&2\\2&1&4&3\\1&2&3&4\end{bmatrix},\ C=\begin{bmatrix}4&2&1&3\\3&1&2&4\\2&4&3&1\\1&3&4&2\end{bmatrix},$$

那么有

$$A,B\rightarrow\begin{bmatrix}\langle 1,4\rangle&\langle 2,3\rangle&\langle 3,2\rangle&\langle 4,1\rangle\\\langle 2,3\rangle&\langle 3,4\rangle&\langle 4,1\rangle&\langle 1,2\rangle\\\langle 3,2\rangle&\langle 4,1\rangle&\langle 1,4\rangle&\langle 2,3\rangle\\\langle 4,1\rangle&\langle 1,2\rangle&\langle 2,3\rangle&\langle 3,4\rangle\end{bmatrix},$$

$$B,C\rightarrow\begin{bmatrix}\langle 4,4\rangle&\langle 3,2\rangle&\langle 2,1\rangle&\langle 1,3\rangle\\\langle 3,3\rangle&\langle 4,1\rangle&\langle 1,2\rangle&\langle 2,4\rangle\\\langle 2,2\rangle&\langle 1,4\rangle&\langle 4,3\rangle&\langle 3,1\rangle\\\langle 1,1\rangle&\langle 2,3\rangle&\langle 3,4\rangle&\langle 4,2\rangle\end{bmatrix},$$

称 A,B 和 B,C 为拉丁方的**并置**. 其中 B 和 C 是正交的拉丁方，而 A 和 B 不是正交的.

正方的拉丁方在实验设计中有着重要的应用. 请看下面的例子.

【例 10.4】 设有两种肥料 A 和 B，每种可能使用的量分别为 1，2，3，4 和 5，则两种肥料的用量组合有 25 种. 假设施用肥料的实验田是正方形的，并被划分成 5 行 5 列的 25 块小正方形. 为了减少土壤条件的影响，要求每行和每列每种肥料至多施用 1 次，问应该怎样安排试验?

解 肥料 A 和 B 分别按照两个正交的拉丁方施用即可. 图10.2 给出了一种方案.

为了研究构造正交拉丁方的方法，我们需要一些有限域上的有限几何的知识.

k 的方程有 n 个，所以不同的线数是 $n^2 + n$.

（3）任取 $AP(F)$ 中的一条线. 若该线的方程是 $y = mx + b, m, b \in F$，则任意给定 $x \in F$，必存在唯一的 y 与之对应，$\langle x, y\rangle$ 就是这条线上的一个点. x 有 n 种可能的取值，得到 n 组 $\langle x, y\rangle$，即线上有 n 个点. 若该线的方程为 $x = k$，对任意的 $y \in F$，$\langle k, y\rangle$ 都是该线上的点，y 有 n 种取值，所以这条线上恰有 n 个点.

（4）任取 $AP(F)$ 中的一点 $\langle a, c\rangle$，则 $x = a$ 是一条过 $\langle a, c\rangle$ 的线. 考虑 $y = mx + b$ 形式的线，若这种线过 $\langle a, c\rangle$ 点，则必满足等式 $c = ma + b$. 对于任意给定的 $m \in F$，可唯一地确定 b，共有 n 种 m, b 满足等式，对应于 n 条过 $\langle a, c\rangle$ 的线. 于是过 $\langle a, c\rangle$ 的线共有 $n + 1$ 条.

∎

【例 10.6】 设 $F = \{0, 1, 2\}$，根据定理 10.2，仿射平面 $AP(F)$ 上有 $3^2 = 9$ 个点，$3^2 + 3 = 12$ 条线，每条线上恰有 3 个点，每个点恰在 4 条线上. 请看图 10.4.

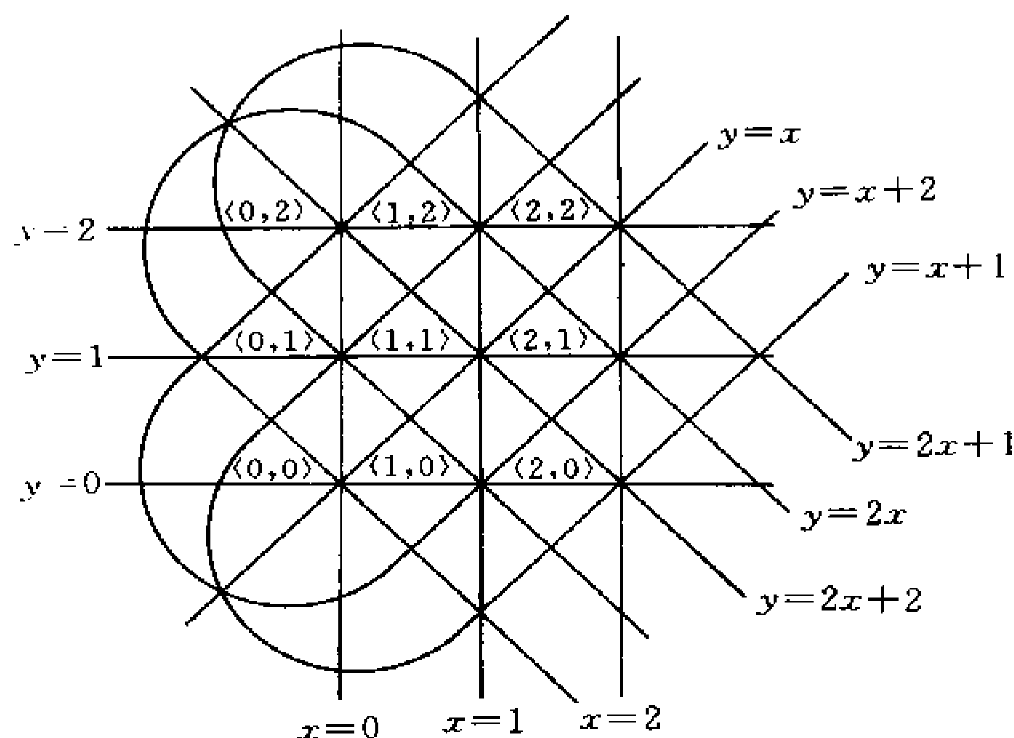


图 10.4

$$x = -c^{-1}e.$$

所以 F 上的线具有下述形式

$$y = mx + b \text{ 或 } x = k,$$

其中 $m,b,k \in F$. 称 m 为线 $y = mx + b$ 的**斜率**.

设 l_1 和 l_2 为 F 上的线,若 l_1 和 l_2 没有公共点,则称 l_1 和 l_2 是**平行**的. 假设 l_1 和 l_2 的方程分别为 $y = m_1x + b_1, y = m_2x + b_2$,则 l_1 与 l_2 平行当且仅当 $m_1 = m_2$ 且 $b_1 \neq b_2$. 这些结果很容易由有限域的知识加以证明,在此不再赘述.

定理 10.1　设 F 为有限域,则 F 上的点和线满足下面的性质:

(1) 过 F 上任意两点可确定一条线;

(2) 任给 F 上的点 P 和线 l,若 P 不在 l 上,则存在 F 上的线 l', l' 过 P 且平行于 l;

(3) 存在 4 个点,其中任意三点都不在同一条线上.

证　(1) 和(2) 的证明留作练习.

(3) 由于 $|F| \geqslant 2$, 存在 $0,1 \in F$, 且 $0 \neq 1$. 则$\langle 0,0\rangle,\langle 0,1\rangle,\langle 1,0\rangle,\langle 1,1\rangle$ 是 4 个点. 其中任何两点都可以确定一条线,而剩下的两个点都不在这条线上. ∎

定义 10.4　设 F 为有限域,称 F 上的点和线所构成的有限几何为 F 所确定的**仿射平面**,记作 $AP(F)$.

关于仿射平面 $AP(F)$ 有下面的定理.

定理 10.2　设 F 是有限域, $|F| = n$,则 $AP(F)$ 满足

(1) 点数为 n^2;

(2) 线数为 $n^2 + n$;

(3) 每条线上恰有 n 个点;

(4) 每个点恰在 $n + 1$ 条线上.

证　(1) 由于 $|F| = n$,则 $|F \times F| = n^2$,所以点数为 n^2.

(2) 每条线由方程 $y = mx + b$ 或 $x = k$ 确定. 由于 m,b 各有 n 种取值,形为 $y = mx + b$ 的方程有 n^2 个. 而 k 有 n 种取值,形为 $x =$

根据定理 10.4 和 10.3 不难得到构造正交拉丁方的方法.

【例 10.7】 令 $F=\{0,1,2\}$,则在 $AP(F)$ 中有两个斜率不为 0 的线平行类,斜率为 1 的线平行类 $A_1=\{y=x,y=x+1,y=x+2\}$ 和斜率为 2 的线平行类 $A_2=\{y=2x,y=2x+1,y=2x+2\}$, A_1 和 A_2 分别确定了两个 3 阶拉丁方 L_1 和 L_2,其中

$$L_1=\begin{bmatrix}3&2&1\\2&1&3\\1&3&2\end{bmatrix},\quad L_1=\begin{bmatrix}3&1&2\\2&3&1\\1&2&3\end{bmatrix}.$$

它们是正交的.

对于有限域 F, $|F|=n\geqslant 3$,通过仿射平面 $AP(F)$ 中的线平行类可以构造出 $n-1$ 个两两正交的 n 阶拉丁方. 而下面的定理告诉我们,通过这种方法得到的 $n-1$ 个拉丁方恰好是所有的两两正交的 n 阶拉丁方.

引理 设 L_1 和 L_2 是正交的 n 阶拉丁方, $\sigma=\begin{pmatrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{pmatrix}$ 是 n 元置换,令 $\sigma(L_1)$ 表示在 L_1 中用 i_j 代替 $j(j=1,2,\cdots,n)$ 以后所得到的结果,则 $\sigma(L_1)$ 也是一个 n 阶拉丁方,且与 L_2 正交.

证 易见 $\sigma(L_1)$ 是一个 n 阶拉丁方. 假设 $\sigma(L_1)$ 与 L_2 不是正交的,必存在 $\langle i_l,j\rangle$ 出现在 $\sigma(L_1)$,L_2 并置的两个位置,从而推出 $\langle l,j\rangle$ 必出现于 L_1,L_2 并置的同样的两个位置. 这与 L_1 与 L_2 是正交的相矛盾. ∎

定理 10.5 设 $L_1,L_2,\cdots,L_k$ 是两两正交的 n 阶拉丁方,则 $k\leqslant n-1$.

证 对 $L_i(i=1,2,\cdots,k)$ 选择 n 元置换 σ_i,使得 $\sigma_i(L_i)$ 的第一行为 $1,2,\cdots,n$. 根据引理, $\sigma_1(L_1),\sigma_2(L_2),\cdots,\sigma_k(L_k)$ 必是两两正交的. 将 $\sigma_i(L_i)$ 的第二行第一列的元素记为 $x_{21}^{(i)}$, $i=1,2,\cdots,k$. 易证对任意的 $i,j\in\{1,2,\cdots,k\}$, $i\neq j$,有 $x_{21}^{(i)}\neq x_{21}^{(j)}$. 假若不然有 $x_{21}^{(i)}=x_{21}^{(j)}$

定义 10.5　设 F 为有限域，A 是 $AP(F)$ 中所有的线构成的集合. R 是 A 上的二元关系，对于任意的 $l_1,l_2 \in A$，$l_1Rl_2 \Leftrightarrow l_1$ 是 l_2 或 l_1 与 l_2 平行，则 R 是 A 上的等价关系. 称关于 R 的等价类为线的平行类.

下面考虑正交拉丁方的构造问题.

定理 10.3　设 $F = \{a_1 = 0, a_2 = 1, a_3, \cdots, a_n\}$ 是有限域，且 $n \geqslant 3$. 任取 $a_i \in F$，$a_i \neq 0$，则

$$\{y = a_i x + a_j \mid j = 1,2,\cdots,n\}$$

确定了 $AP(F)$ 中的一个线平行类. 将线 $y = a_i x + a_j$ 上的点标记为 j，$j = 1,2,\cdots,n$，则该平行类中所有点的标记构成一个拉丁方.

证　由定理 10.2，对于给定的 $a_i, a_j \in F$，$a_i \neq 0$，线 $y = a_i x + a_j$ 上恰有 n 个点. 这 n 个点的横坐标构成了 F 中的全体元素，纵坐标也构成了 F 中的全体元素，即 $AP(F)$ 上的每行每列恰含有 1 个点. 这就证明在标记阵列中每行每列恰含有 1 个 j. 由于平行类 $\{y = a_i x + a_j \mid j = 1,2,\cdots,n\}$ 中有 n 条彼此不交的线，分别对应于 $j = 1,2,\cdots,n$，因此 $1,2,\cdots,n$ 中的每个数在标记阵列中的每行每列恰好出现 1 次. ∎

定理 10.4　设 F 为有限域，并且 $|F| \geqslant 3$. 令 $L_1, L_2, \cdots, L_{n-1}$ 是对应于 $AP(F)$ 中 $n-1$ 个斜率不为 0 的线平行类的拉丁方，则 $\forall L_i, L_j$，$i,j \in \{1,2,\cdots,n-1\}$，$i \neq j$，$L_i$ 和 L_j 是正交的.

证　设 $F = \{a_1 = 0, a_2 = 1, a_3, \cdots, a_n\}$，$AP(F)$ 的两个线平行类 A_1 和 A_2 的斜率分别为 m_1 和 m_2，m_1 和 m_2 都不为 0 且 $m_1 \neq m_2$，对应于 A_1 和 A_2 的两个拉丁方分别为 L_1 和 L_2. 假若 L_1 和 L_2 不是正交的，则存在有序对 $\langle i, j \rangle$，$i,j \in \{1,2,\cdots,n\}$，出现于 L_1，L_2 并置的两个位置，即如果 i 出现于 L_1 的两个位置，则 j 出现于 L_2 中同样的两个位置. 由定理 10.3 的证明可知在仿射平面 $AP(F)$ 中线 $y = m_1 x + a_i$ 和 $y = m_2 x + a_j$ 必交于两点. 这与定理 10.1 中两点确定一条线相矛盾. ∎

$$C_1 = \begin{bmatrix} \langle 3,B_1\rangle & \langle 2,B_1\rangle & \langle 1,B_1\rangle \\ \langle 2,B_1\rangle & \langle 1,B_1\rangle & \langle 3,B_1\rangle \\ \langle 1,B_1\rangle & \langle 3,B_1\rangle & \langle 2,B_1\rangle \end{bmatrix}.$$

类似地，由 A_2 和 B_2 可以构造另一个 12 阶的方阵 C_2. C_1 和 C_2 的各项都是 $\langle i,j\rangle$ 形式，其中 $i=1,2,3$，$j=1,2,3,4$. 然后对这 12 个有序对分别标记整数 1,2,…,12，使得不同的有序对的标记也不相同，从而得到两个标记阵列 L_1 和 L_2. 由阵列 C_1 和 C_2 的构成可知，它的每行每列的有序对不是第一个元素不等就是第二个元素不等，因此在每行和每列中每个有序对恰好出现一次. 这就证明了 L_1 和 L_2 都是拉丁方.

下面证明 L_1 和 L_2 是正交的. 假若不然，则存在有序对 $\langle\langle u,v\rangle,\langle w,t\rangle\rangle$ 出现在 C_1，C_2 并置的两个位置. 根据 C_1 和 C_2 的构成可知或者有 $\langle u,w\rangle$ 出现于 A_1，A_2 并置的两个位置或者有 $\langle v,t\rangle$ 出现于 B_1，B_2 并置的两个位置，这都和 A_1，A_2 以及 B_1，B_2 的正交性矛盾.

不难看到，这种构造高阶正交拉丁方的方法是普遍适用的. 对于正整数 n，

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

为 n 的素因子分解式，其中 p_i 为素数，$\alpha_i \in Z^+$，$i=1,2,\cdots,t$. 如果不存在 $p_i^{\alpha_i}=2$，那么对任意的 $i=1,2,\cdots,t$，都存在正交的 $p_i^{\alpha_i}$ 阶的拉丁方. 使用上面的构造方法，可顺序构造出 $p_1^{\alpha_1}p_2^{\alpha_2}$ 阶，$p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$，…，$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ 阶正交的拉丁方. 这就证明了只要 n 不是某个奇数的 2 倍都可以构造出 n 阶的正交拉丁方.

进一步的研究已经证明，如果 n 是某个奇数的 2 倍，但 $n \neq 2$ 和 6，也存在着 n 阶的正交的拉丁方，并且给出了构造的方法. 限于篇幅，这里不再加以详细介绍.

§10.2　t-设计

本节主要研究不完全的设计. 先引入一些基本概念.

定义 10.6　设 $X=\{x_1,x_2,\cdots,x_v\}$ 是点的集合，$B=\{B_1,B_2,$

$=t$，则有序对 $\langle t,t\rangle$ 出现于 $\sigma_i(L_i)$，$\sigma_j(L_j)$ 并置的第二行第一列和第一行第 t 列的两个位置，与 $\sigma_i(L_i)$，$\sigma_j(L_j)$ 是正交的相矛盾. 由于 $x_{21}^{(1)}$，$\cdots$，$x_{21}^{(k)}$ 彼此不等，且它们都不为 1，至多只能有 $n-1$ 个，从而证明了 $k\leqslant n-1$. ∎

回顾 §4.3（有限域上的多项式环），我们已经知道，对于任何正整数 n，存在着有限域 $F(|F|=n)$ 当且仅当 n 是某个素数的幂. 因此当 $n=p^t$，p 为素数且 $n\geqslant 3$ 时，可以利用仿射平面 $AP(F)$ 构造 $n-1$ 个两两正交的 n 阶拉丁方. 对于其它的 n，当 $n=2$ 或 6 时，不存在着正交的拉丁方，剩下的 n 都存在着正交的拉丁方. 下面给出一种方法，可以从一对 n_1 阶正交的拉丁方和一对 n_2 阶正交的拉丁方构造出一对 n_1n_2 阶的正交拉丁方. 请看下面的例子.

设 $n_1=3$，$n_2=4$，A_1，A_2 是一对 3 阶的正交拉丁方，B_1，B_2 是一对 4 阶的正交拉丁方.

$$A_1=\begin{bmatrix}3&2&1\\2&1&3\\1&3&2\end{bmatrix},\qquad A_2=\begin{bmatrix}3&1&2\\2&3&1\\1&2&3\end{bmatrix},$$

$$B_1=\begin{bmatrix}4&3&2&1\\3&4&1&2\\2&1&4&3\\1&2&3&4\end{bmatrix},\qquad B_2=\begin{bmatrix}4&2&1&3\\3&1&2&4\\2&4&3&1\\1&3&4&2\end{bmatrix}.$$

如下构造 12 阶正交的拉丁方. 对于 A_1 中的每一项 a，用下面的 4×4 阵列来代替

$$\langle a,B_1\rangle=\begin{bmatrix}\langle a,4\rangle&\langle a,3\rangle&\langle a,2\rangle&\langle a,1\rangle\\\langle a,3\rangle&\langle a,4\rangle&\langle a,1\rangle&\langle a,2\rangle\\\langle a,2\rangle&\langle a,1\rangle&\langle a,4\rangle&\langle a,3\rangle\\\langle a,1\rangle&\langle a,2\rangle&\langle a,3\rangle&\langle a,4\rangle\end{bmatrix},$$

从而得到一个 12 阶的方阵 C_1

定义 10.7　设 $X=\{x_1,x_2,\cdots,x_v\}$，$B=\{B_1,B_2,\cdots,B_b\}$ 是 X 的子集族，X 和 B 构成一个 t-(v,k,λ) 设计，则这个 t- 设计的**相交矩阵** $M=(a_{ij})$ 是 v 行 b 列的(0-1) 矩阵，其中

$$a_{ij}=\begin{cases}1, & 若\ x_i \in B_j,\\ 0, & 若\ x_i \notin B_j.\end{cases}$$

【例 10.9】　例 10.8 中的头两个 t- 设计的相交矩阵分别是：

$$\underset{(1)}{\begin{bmatrix}1&0&0&1\\1&1&0&0\\0&1&1&0\\0&0&1&1\end{bmatrix}},\qquad \underset{(2)}{\begin{bmatrix}1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\\1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}}.$$

定义 10.8　(1) $k<v$ 的 2-(v,k,λ) 设计称为**均衡的不完全的区组设计**(Balanced Incompleted Block Design)，简称 **BIBD**.

(2) $b=v$ 的 t-(v,k,λ) 设计称为**方设计**或**对称设计**.

(3) $\lambda=1$ 的 t-$(v,k,1)$ 设计称为 **Steiner 系统**.

(4) $\lambda=1$ 的对称的 BIBD 称为**射影平面**. 令 $n=k-1$，称 n 为该射影平面的**阶**.

【例 10.10】　例 10.8 中(2)的设计是一个 BIBD. (1) 和(2) 的设计是对称设计. (2) 和(3) 的设计是 Steiner 系统. 而(2) 的设计是射影平面，实际上它就是 **Fano 平面**，是唯一的 2 阶射影平面. Fano 平面的定义如下：

设 $X=\{0,1,\cdots,6\}$，

$B=\{\{x,x\oplus 1,\ x\oplus 3\}\mid x\in X\}$.

其中 $\oplus$ 为模 7 加法. 则 X,B 构成一个 2-(7,3,1) 设计. 图 10.7 就是

$\cdots,B_b\}$ 是 X 的子集族，称为块的集合，其中 $|B_i|=k,i=1,2,\cdots,b$. 如果对于 X 的任何 t 元子集 $T(k\geqslant t)$ 恰好存在着 λ 个块与 T 中所有的点都相交，则称 X 和 B 构成了一个 v 个点，块大小为 k，指数为 λ 的 t 设计，简记为 t-(v,k,λ) 设计.

【例 10.8】

(1) $X=\{1,2,3,4\}$，$B=\{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}$，则 X，B 构成一个 1-(4,2,2) 设计；

(2) $X=\{1,2,3,4,5,6,7\}$，$B=\{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}$，则 X,B 构成一个 2-(7,3,1) 设计；

(3) 设 X 为完全五边形 K_5 的边集，图 10.5 中三种类型的边集作为块，则(1) 型块有 $\binom{5}{1}=5$ 块，(2) 型块有 $\binom{5}{3}=10$ 块，(3) 型块有 $3\binom{5}{1}=15$ 块，共计 30 个块. 任取 K_5 的 3 条边 e_1,e_2,e_3，在同构的意义下可能的取法如图 10.6. 在情况(a)，这 3 条边只能与(1) 型的一个块相交. 在情况(b)，这 3 条边只能与(3) 型的一个块相交. 在情况(c)和(d)，这 3 条边只能与(2) 型的一个块相交. 所以 X 和这 30 个块的集合 B 构成一个 3-(10,4,1) 设计.

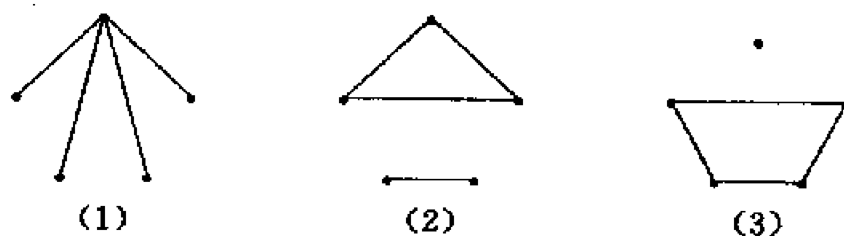


图 10.5

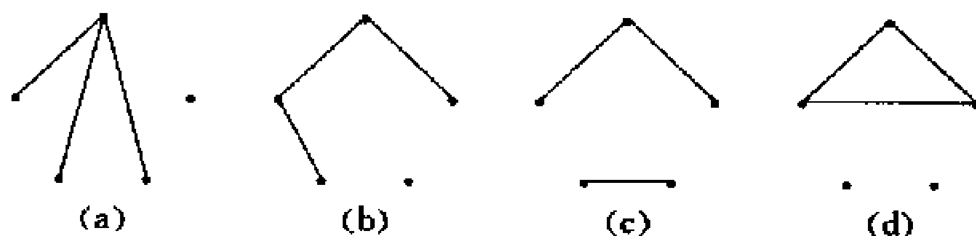


图 10.6

推论 3　设 D 为一个 n 阶的射影平面，则

$$v = n^2 + n + 1.$$

证　由于射影平面是一个对称的 BIBD，由推论 2 有

$$\lambda(v-1) = k(k-1).$$

将 $\lambda = 1, n = k-1$ 代入，命题得证. ∎

定理 10.7　设 X,B 构成一个 t-(v,k,λ) 设计，则对任意的 i，$0 \leqslant i \leqslant t$，与 X 的一个给定的 i 子集的所有点相交的块数是

$$b_i = \lambda\binom{v-i}{t-i}\Big/\binom{k-i}{t-i}. \tag{10.2}$$

证　设 A 是 X 的一个 i 子集，即 $|A| = i$. 取 X 的一个 t 子集 T，使得 $A \subseteq T$. 令 B_j 是与 T 的所有点相交的块，计数有序对 $\langle T, B_j\rangle$ 的个数. 一方面 t 子集数为 $\binom{v-i}{t-i}$，与某个 T 相交的块数为 λ. 所以不同的有序对 $\langle T, B_j\rangle$ 有 $\lambda\binom{v-i}{t-i}$ 个. 另一方面，与 A 中所有的点相交的块数为 b_i. 而对每个块，从中选出 t 个点并使得 A 的 i 个点在内的方法有 $\binom{k-i}{t-i}$ 种，所以有 $b_i\binom{k-i}{t-i}$ 个不同的有序对 $\langle T, B_j\rangle$. 等式得证. ∎

推论 1　设 X,B 构成一个 2-(v,k,λ) 设计，则与 X 中一个点相交的块数 r 满足

(1) $\lambda(v-1) = r(k-1)$; (10.3)

(2) $bk = vr$. (10.4)

证　(1) 将 $t=2, i=1$ 代入 10.2 式得

$$r = b_1 = \lambda\binom{v-1}{1}\Big/\binom{k-1}{1} = \lambda(v-1)/(k-1).$$

(2) 由

$$b = b_0 = \lambda\binom{v}{2}\Big/\binom{k}{2}$$

Fano 平面的示意图. 图上的点就是 X 中的点. 而每条线是 B 中的块，其中有 6 条直线，分别对应块 $\{0,1,3\}$，$\{2,3,5\}$，$\{3,4,6\}$，$\{4,5,0\}$，$\{5,6,1\}$，$\{6,0,2\}$. 另一条是以 0 为圆心的圆，对应于块 $\{1,2,4\}$.

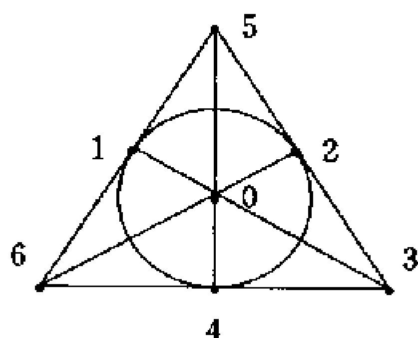


图 10.7

下面的定理给出了一个 t-(v,k,λ) 设计存在的必要条件.

定理 10.6　一个 t-(v,k,λ) 设计存在的必要条件是

$$b\binom{k}{t}=\lambda\binom{v}{t}. \tag{10.1}$$

证　设集合 X 和 X 的子集族 B 构成 t-(v,k,λ) 设计. 对于 X 的 t-元子集 T，做有序对 $\langle T,B_i\rangle$，其中 B_i 是与 T 中所有的点相交的块. 用两种方法计数所有的有序对 $\langle T,B_i\rangle$. 一方面，不同的 T 子集数为 $\binom{v}{t}$，与某个 T 子集相交的块数为 λ，故有序对数为 $\lambda\binom{v}{t}$. 另一方面，B 中有 b 个块，而每个块恰与 $\binom{k}{t}$ 个 T 子集相交，故有序对数为 $b\binom{k}{t}$，从而证明了 $b\binom{k}{t}=\lambda\binom{v}{t}$. ∎

推论 1　1-(v,k,λ) 设计满足 $kb=\lambda v$.

证　将 $t=1$ 代入 10.1 式即可. ∎

推论 2　设 D 为一个对称的 BIBD，则

$$\lambda(v-1)=k(k-1).$$

证　将 $t=2$ 代入 10.1 式得

$$b\binom{k}{2}=\lambda\binom{v}{2},$$

即

$$bk(k-1)=\lambda v(v-1).$$

由于 $b=v$，则等式得证. ∎

由于 M 是 BIBD 的相交矩阵,必有 λ 个块与 $\{x_i, x_j\}$ 相交,所以当 $i \neq j$ 时在 MM^T 的 i 行 j 列元素为 λ. ∎

定理 10.8 设 D 是一个 BIBD,则 $b \geqslant v$.

证 由于 D 是 BIBD,$v > k$,由 10.3 式有 $r > \lambda$.

假设 $b < v$,在矩阵 M 中加上 $v-b$ 个全 0 的列,得到一个 v 行 v 列的方阵 M_1. 易见 $MM^T = M_1M_1^T$. 令 $\det A$ 表示 A 的行列式,则有

$$\det MM^T = \det M_1M_1^T = \det M_1 \cdot \det M_1^T = 0.$$

由引理有

$$\det MM^T = \det \begin{bmatrix} r & \lambda & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & \lambda & r & \cdots & \lambda \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & \lambda & \lambda & \lambda & \cdots & r \end{bmatrix}$$

$$= \det \begin{bmatrix} r & \lambda - r & \lambda - r & \lambda - r & \cdots & \lambda - r \\ \lambda & r - \lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r - \lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & 0 & 0 & 0 & \cdots & r - \lambda \end{bmatrix}$$

$$= \det \begin{bmatrix} r + (v-1)\lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & r - \lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r - \lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & 0 & 0 & 0 & \cdots & r - \lambda \end{bmatrix}$$

得

$$b = \lambda v(v-1)/k(k-1).$$

将 10.3 式代入等式得证. ∎

推论 2 若 X,B 构成一个 $2\text{-}(v,3,1)$ 设计(Steiner 三元系统),则

(1) $r = (v-1)/2$. (10.5)

(2) $b = v(v-1)/6$. (10.6)

证 (1) 将 $k=3,\lambda=1$ 代入 10.3 式即可.

(2) 将 $k=3$ 和 10.5 式代入 10.4 式即可. ∎

推论 3 若 X,B 构成一个 $2\text{-}(v,3,1)$ 设计(Steiner 三元系统),则 v 只可能等于 $3,6n+1$ 或 $6n+3$,其中 n 是某个正整数.

证 由 10.5 式得 $v=2r+1, r\in Z^+$. 因此必有 $v\geqslant 3$ 且 v 是奇数,即 $v\neq 4,6n,6n+2$ 和 $6n+4$.

若 $v=6n+5, n\in N$,则由 10.6 式得 $b=10/3+n', n'$ 是整数,与 b 是整数矛盾. ∎

可以证明推论 3 的条件是 Steiner 三元系统存在的充分必要条件. 限于篇幅,不再赘述.

下面的定理给出了 BIBD 存在的另一个必要条件(**Fisher 不等式**),为此我们先给出一个引理.

引理 设 $X=\{x_1,x_2,\cdots,x_v\}, B=\{B_1,B_2,\cdots,B_b\}$ 构成一个 BIBD,M 是该设计的相交矩阵,M^T 为 M 的转置,则在矩阵 MM^T 的主对角线上的元素都是 r,其它的元素都是 λ.

证 令 $M=(a_{ij}), M^T=(a_{ij}')$. 对任意 $i=1,2,\cdots,v$,

$x_i\in B_s \Leftrightarrow a_{is}=1$ 且 $a'_{si}=1 \Leftrightarrow$ 在 MM^T 的 i 行 i 列位置加一个 1. 由于与 x_i 相交的块数是 r,所以在 MM^T 的 i 行 i 列元素也是 r.

对任意的 $i,j=1,2,\cdots,v, i\neq j$,

$$x_i,x_j\in B_s \Leftrightarrow a_{is}=1 \text{ 且 } a'_{sj}=1$$

$$\Leftrightarrow \text{在 } MM^T \text{ 的 } i \text{ 行 } j \text{ 列的位置加一个 } 1.$$

因此恰有 B 中的 λ 个块与 T 相交. 任取其中的块 B_j，则 $I \subseteq B_j$，且 $B'_j = B_j - I$ 与 T' 相交. 从而证明 B' 中有 λ 个块与 T' 相交. 假若有另外的块 $B'_l \in B'$ 也与 T' 相交，那么 $B'_l \cup I = B_l$ 也与 T 相交，则与 T 相交的块数至少为 $\lambda + 1$，与 D 是 t-(v,k,λ) 设计矛盾. ▮

定义 10.9　令 X,B,I,D,X',B' 如定理 10.9 所述，则 X' 和 B' 构成的 $(t-i)$-$(v-i,k-i,\lambda)$ 设计称为 **D 导出的设计**，记作 D_I.

【例 10.12】　设 $X = \{1,2,\cdots,10\}$，B 中有 30 个块，依次列在下边：

$\{1,2,3,9\},\{1,2,4,6\},\{1,2,5,8\},\{1,2,7,10\},\{1,3,4,8\},$
$\{1,3,5,10\},\{1,3,6,7\},\{1,4,5,7\},\{1,4,9,10\},\{1,5,6,9\},$
$\{1,6,8,10\},\{1,7,8,9\},\{2,3,4,10\},\{2,3,5,7\},\{2,3,6,8\},$
$\{2,4,5,9\},\{2,4,7,8\},\{2,5,6,10\},\{2,6,7,9\},\{2,8,9,10\},$
$\{3,4,5,6\},\{3,4,7,9\},\{3,5,8,9\},\{3,6,9,10\},\{3,7,8,10\},$
$\{4,5,8,10\},\{4,6,8,9\},\{4,6,7,10\},\{5,6,7,8\},\{5,7,9,10\},$

则 X,B 构成一个 3-(10,4,1) 设计 D. 令 $I = \{10\}$，则

$X' = \{1,2,\cdots,9\},$

$B' = \{\{1,2,7\},\{1,3,5\},\{1,4,9\},\{1,6,8\},\{2,3,4\},\{2,5,6\},$
$\{2,8,9\},\{3,6,9\},\{3,7,8\},\{4,5,8\},\{4,6,7\},\{5,7,9\}\}$

构成一个 2-(9,3,1) 设计，是 D 导出的设计.

引理　设 $X = \{x_1,x_2,\cdots,x_v\}$，$B = \{B_1,B_2,\cdots,B_v\}$ 构成一个对称的 2-(v,k,λ) 设计，则对任意的 $B_i,B_j \in B$，$i \neq j$，B_i 与 B_j 恰含有 λ 个公共点.

证　任取 $B_i \in B$，设 a_j 是除 B_i 以外与 B_i 有 j 个公共点的块的个数，$1 \leqslant j \leqslant k$，则

$$\sum_{j=0}^{k} a_j = v - 1. \qquad ①$$

设 x 是 B_i 中的点，B_l 是和点 x 相交的块，且 $l \neq i$，计数所有的有序对 $\langle x, B_l\rangle$. 一方面由于和 x 相交的块数为 r，除去 B_i 后应是 $r-1$，

$$= [r + (v - 1)\lambda](r - \lambda)^{v-1},$$

所以有

$$[r + (v - 1)\lambda](r - \lambda)^{v-1} = 0.$$

这与 $r > \lambda$ 且 $r, v - 1, \lambda$ 都是正整数矛盾. ∎

推论 设 D 为一个对称的BIBD，v 为偶数，则 $k - \lambda$ 是平方数.

证 由定理 10.8 的证明可知

$$\det MM^T = [r + (v - 1)\lambda](r - \lambda)^{v-1},$$

其中 M 为 D 的相交矩阵. 由于 D 是对称设计，$\det M = \det M^T$，因此有

$$[\det M]^2 = [r + (v - 1)\lambda](r - \lambda)^{v-1}.$$

由定理10.6的推论2知 $\lambda(v - 1) = k(k - 1)$，又由10.4式有 $r = k$，代入上式得

$$[\det M]^2 = k^2(k - \lambda)^{v-1}.$$

因为 v 为偶数，所以 $k - \lambda$ 为平方数. ∎

【例 10.11】 证明不存在对称的 2-(8,7,4) 设计.

证 $v = 8, k = 7, \lambda = 4$，$v$ 是偶数，$k - \lambda = 3$ 不是平方数，由定理 10.8 的推论得证. ∎

对于给定的正整数 v, k, λ, t，判定是否存在 t-(v, k, λ) 设计这一问题至今并没有得到根本的解决，只得到了某些特殊情况下的必要条件或充分条件. 下面考虑构造 t-(v, k, λ) 设计的问题.

定理 10.9 设 $X = \{x_1, x_2, \cdots, x_v\}$，$B = \{B_1, B_2, \cdots, B_b\}$，$D$ 是 X 和 B 构成的 t-(v, k, λ) 设计，$I \subseteq X$ 且 $|I| = i$. 令

$$X' = X - I, B' = \{B_j - I \mid B_j \in B \text{ 且 } I \subseteq B_j\},$$

则 X', B' 构成一个 $(t - i)$-$(v - i, k - i, \lambda)$ 设计.

证 显然 $|X'| = |X| - |I| = v - i$，且 B' 块的大小为 $k - i$. 对于任意 $T' \subseteq X'$，$|T'| = t - i$，令 $T = T' \cup I$. 因 $T' \cap I = \varnothing$，则

$$|T| = |T'| + |I| = t - i + i = t.$$

B, B_j 与 B_i 恰有 λ 个公共点，故 $|B_j - B_i| = k - \lambda$. 对任何 $x, y \in X'$，恰有 λ 个块 $B_{l_1}, B_{l_2}, \cdots, B_{l_\lambda}$ 含有 x, y，所以恰有 λ 个块 $B_{l_1} - B_i$，$B_{l_2} - B_i, \cdots, B_{l_\lambda} - B_i \in B'$ 且含有 x, y，从而证明了 X', B' 构成一个2-$(v-k, k-\lambda, \lambda)$ 设计.

【例 10.13】 设 $X = \{0,1,3,\cdots,6\}, B = \{\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\}\}$ 构成一个对称的 2-(7,3,1) 设计. 取 $B_i = \{0,1,3\}$，则 $X' = \{2,4,5,6\}, B' = \{\{2,4\},\{2,5\},\{4,6\},\{4,5\},\{5,6\},\{6,2\}\}$ 构成一个 2-(4,2,1) 设计.

定理 10.11 设 $X = \{x_1, x_2, \cdots, x_v\}, B = \{B_1, B_2, \cdots, B_v\}$ 构成一个对称的 2-(v,k,λ) 设计，$\lambda > 1$. 任取 $B_i \in B$，令

$$X' = B_i, B' = \{B_j \cap B_i \mid B_j \in B \text{ 且 } B_j \neq B_i\},$$

则 X', B' 构成一个 2-$(k, \lambda, \lambda - 1)$ 设计.

证 显然 $|X'| = k$. 由定理 10.10 的引理，对任意的 $B_j \in B, B_j \neq B_i$，B_j 与 B_i 恰有 λ 个公共点，所以 B' 中每个块的大小为 λ.

对任意的 $x, y \in X'$，恰有 λ 个块 $B_{l_1}, B_{l_2}, \cdots, B_{l_\lambda} \in B$ 含有 x, y. 除了 B_i 以外，正好有 $\lambda - 1$ 个块含有 x, y. 因此 B' 中恰有 $\lambda - 1$ 个块含有 x, y. 这就证明了 X', B' 构成了一个 2-$(k, \lambda, \lambda - 1)$ 设计. ∎

【例 10.14】 设 $X = \{1,2,3,4\}, B = \{\{1,2,3\},\{2,3,4\},(3,4,1\},(4,1,2\}\}$，则 X, B 构成一个对称的 2-(4,3,2) 设计. 取 $B_i = \{1,2,3\}$，则 $X' = \{1,2,3\}$. $B' = \{\{2,3\},\{1,3\},\{1,2\}\}$，$X', B'$ 构成一个 2-(3,2,1) 设计.

2-$(v,3,1)$ 设计称作 Steiner 三元系统. 下面的定理说明如何由已知的分别含 v_1 个点和 v_2 个点的 Steiner 三元系统 S_1 和 S_2 构造一个含 $v_1 v_2$ 个点的 Steiner 三元系统 S.

定理 10.12 设 $X_1 = \{x_1, x_2, \cdots, x_{v_1}\}$，$X_1$ 与 B_1 构成 Steiner 三元系统；$X_2 = \{y_1, y_2, \cdots, y_{v_2}\}$，$X_2, B_2$ 也构成 Steiner 三元系统. 则存在一个点集为 X，块集为 B 的 Steiner 三元系统且 $|X| = v_1 v_2$.

证 令 $X = \{z_{ij} \mid i = 1, 2, \cdots, v_1 \text{ 且 } j = 1, 2, \cdots, v_2\}$，则

因此有序对数应是 $k(r-1)=k(k-1)$,(对称设计的 $k=r$). 另一方面,$\sum_{j=0}^{k} ja_j$ 也计数了有序对 $\langle x,B_l\rangle$,故有

$$\sum_{j=0}^{k} ja_j = k(k-1). \qquad ②$$

设 $x,y\in B_i$,B_l 是除 B_i 以外和 x,y 相交的块,计数有序三元组 $\langle x,y,B_l\rangle$. 一方面 B 中和 x,y 相交的块恰有 λ 个,除去 B_i,有 $\lambda-1$ 个,所以有 $\binom{k}{2}(\lambda-1)$ 个三元组 $\langle x,y,B_l\rangle$. 另一方面,$\binom{j}{2}a_j$ 计数了和 B_i 有 j 个公共点,并且其中包含 x,y 两点的 $\langle x,y,B_l\rangle$ 个数,故有

$$\sum_{j=0}^{k}\binom{j}{2}a_j = \binom{k}{2}(\lambda-1). \qquad ③$$

由 ①,② 和 ③ 式推出

$$\sum_{j=0}^{k}(j-\lambda)^2a_j = \sum_{j=0}^{k}(j^2-j+j-2j\lambda+\lambda^2)a_j$$

$$=\sum_{j=0}^{k} j(j-1)a_j + \sum_{j=0}^{k}(1-2\lambda)ja_j + \lambda^2\sum_{j=0}^{k}a_j$$

$$=k(k-1)(\lambda-1)+(1-2\lambda)k(k-1)+\lambda^2(v-1)$$

$$=k(k-1)(-\lambda)+\lambda^2(v-1)$$

$$=\lambda[\lambda(v-1)-k(k-1)]$$

$$=0, \qquad (\text{由 } 10.3 \text{ 式和 } r=k).$$

这就证明了只有当 $j=\lambda$ 时,$a_j\neq 0$,其余 a_j 都为 0,因此任何和 B_i 相交的块恰好与 B_i 交于 λ 个点. ∎

定理 10.10 设 $X=\{x_1,x_2,\cdots,x_v\}$,$B=\{B_1,B_2,\cdots,B_v\}$ 构成一个对称的 2-(v,k,λ) 设计. 对任意的 $B_i\in B$,令

$$X'=X-B_i, B'=\{B_j-B_i \mid B_j\in B \text{ 且 } B_j\neq B_i\},$$

则 X',B' 构成一个 2-$(v-k,k-\lambda,\lambda)$ 设计.

证 显然 $|X'|=|X|-|B_i|=v-k$. 由引理,对任何 $B_j\in$

B，B_j与B_i恰有λ个公共点，故$|B_j - B_i| = k - \lambda$. 对任何$x,y \in X'$，恰有$\lambda$个块$B_{l_1}, B_{l_2}, \cdots, B_{l_\lambda}$含有$x,y$，所以恰有$\lambda$个块$B_{l_1} - B_i$，$B_{l_2} - B_i, \cdots, B_{l_\lambda} - B_i \in B'$且含有$x,y$，从而证明了$X',B'$构成一个$2\text{-}(v-k, k-\lambda, \lambda)$设计.

【例 10.13】 设$X = \{0,1,3,\cdots,6\}$，$B = \{\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\}\}$构成一个对称的$2\text{-}(7,3,1)$设计. 取$B_i = \{0,1,3\}$，则$X' = \{2,4,5,6\}$，$B' = \{\{2,4\},\{2,5\},\{4,6\},\{4,5\},\{5,6\},\{6,2\}\}$构成一个$2\text{-}(4,2,1)$设计.

定理 10.11 设$X = \{x_1,x_2,\cdots,x_v\}$，$B = \{B_1,B_2,\cdots,B_v\}$构成一个对称的$2\text{-}(v,k,\lambda)$设计，$\lambda > 1$. 任取$B_i \in B$，令

$$X' = B_i, B' = \{B_j \cap B_i | B_j \in B \text{ 且 } B_j \neq B_i\},$$

则X',B'构成一个$2\text{-}(k,\lambda,\lambda-1)$设计.

证 显然$|X'| = k$. 由定理 10.10 的引理，对任意的$B_j \in B$，$B_j \neq B_i$，B_j与B_i恰有λ个公共点，所以B'中每个块的大小为λ.

对任意的$x,y \in X'$，恰有λ个块$B_{l_1}, B_{l_2}, \cdots, B_{l_\lambda} \in B$含有$x,y$. 除了$B_i$以外，正好有$\lambda - 1$个块含有$x,y$. 因此$B'$中恰有$\lambda - 1$个块含有$x,y$. 这就证明了$X',B'$构成了一个$2\text{-}(k,\lambda,\lambda-1)$设计. ∎

【例 10.14】 设$X = \{1,2,3,4\}$，$B = \{\{1,2,3\},\{2,3,4\},\{3,4,1\},\{4,1,2\}\}$，则$X,B$构成一个对称的$2\text{-}(4,3,2)$设计. 取$B_i = \{1,2,3\}$，则$X' = \{1,2,3\}$. $B' = \{\{2,3\},\{1,3\},\{1,2\}\}$，$X',B'$构成一个$2\text{-}(3,2,1)$设计.

$2\text{-}(v,3,1)$设计称作 Steiner 三元系统. 下面的定理说明如何由已知的分别含v_1个点和v_2个点的 Steiner 三元系统S_1和S_2构造一个含v_1v_2个点的 Steiner 三元系统S.

定理 10.12 设$X_1 = \{x_1,x_2,\cdots,x_{v_1}\}$，$X_1$与$B_1$构成 Steiner 三元系统；$X_2 = \{y_1,y_2,\cdots,y_{v_2}\}$，$X_2$，$B_2$也构成 Steiner 三元系统. 则存在一个点集为X，块集为B的 Steiner 三元系统且$|X| = v_1v_2$.

证 令$X = \{z_{ij} | i = 1, 2, \cdots, v_1 \text{ 且 } j = 1, 2, \cdots, v_2\}$，则

$|X| = v_1 v_2$. 对于任意的 $z_{ab}, z_{cd}, z_{ef} \in X$,

$$\begin{aligned}
&\{z_{ab}, z_{cd}, z_{ef}\} \in B \\
\Leftrightarrow\ &(b = d = f \text{ 且 } \{x_a, x_c, x_e\} \in B_1) \\
&\text{或}(a = c = e \text{ 且 } \{y_b, y_d, y_f\} \in B_2) \\
&\text{或}(\{x_a, x_c, x_e\} \in B_1 \text{ 且 } \{y_b, y_d, y_f\} \in B_2).
\end{aligned}$$

易见 B 中的块大小为 3.

任取 $z_{mn}, z_{pq} \in X$,若 $m = p$,由 $y_n, y_q \in X_2$ 且 X_2, B_2 构成Steiner三元系统,必存在唯一的 $\{y_n, y_q, y_l\} \in B_2$ 包含 y_n, y_q 点,则 $\{z_{mn}, z_{pq}, z_{ml}\}$ 是唯一的含 z_{mn}, z_{pq} 的块.

若 $n = q$,同上面的情况类似可证.

若 $m \neq p, n \neq q$,则 $x_m, x_p \in X_1, y_n, y_q \in X_2$. 由于 X_1, B_1 和 X_2, B_2 都构成Steiner三元系统,必存在唯一的 $\{x_m, x_p, x_j\} \in B_1$ 含有 x_m, x_p 以及唯一的 $\{y_n, y_q, y_l\} \in B_2$ 含有 y_n, y_q,因此 $\{z_{mn}, z_{pq}, z_{jl}\}$ 是 B 中唯一的含 z_{mn}, z_{pq} 的三元组,从而得到 $\lambda = 1$.

综上所述,X, B 构成一个 $v_1 v_2$ 个点的 Steiner 三元系统. ∎

【例10.15】 设 $X_1 = X_2 = \{1,2,3\}$, $B_1 = B_2 = \{\{1,2,3\}\}$,则 X_1, B_1 以及 X_2, B_2 都构成 2-(3,3,1) 设计,即 Steiner 三元组.

$$\begin{aligned}
\text{令 } X = \{&z_{11}, z_{12}, z_{13}, z_{21}, z_{22}, z_{23}, z_{31}, z_{32}, z_{33}\}, \\
B = \{&\{z_{11}, z_{12}, z_{13}\}, \{z_{21}, z_{22}, z_{23}\}, \{z_{31}, z_{32}, z_{33}\}, \\
&\{z_{11}, z_{21}, z_{31}\}, \{z_{12}, z_{22}, z_{32}\}, \{z_{13}, z_{23}, z_{33}\}, \\
&\{z_{11}, z_{22}, z_{33}\}, \{z_{11}, z_{23}, z_{32}\}, \{z_{12}, z_{21}, z_{33}\}, \\
&\{z_{12}, z_{23}, z_{31}\}, \{z_{13}, z_{21}, z_{32}\}, \{z_{13}, z_{22}, z_{31}\}\}.
\end{aligned}$$

则 X, B 构成一个 2-(9,3,1) 设计,即 9 个点的 Steiner 三元系统.

考虑上一节的有限域 F 上的仿射平面 $AP(F)$. 若 $|F| = n$,则 $AP(F)$ 上恰有 n^2 个点,$n^2 + n$ 条线,每条线上恰有 n 个点,并且每个点恰在 $n+1$ 条线上. 如果把这 n^2 个点看作设计中的点,线看作设计中的块,则在 $AP(F)$ 中任意两点唯一地确定一条线. 即对该设计中的任何两个点只有唯一的块与它们相交,因此仿射平面 $AP(F)$ 构成

一个 2-$(n^2,n,1)$ 设计. 比较例 10.6 和例 10.15,如果令仿射平面中的点与设计中的点建立如下的对应:

$$\langle 0,2\rangle \mapsto z_{11},\quad \langle 1,2\rangle \mapsto z_{12},\quad \langle 2,2\rangle \mapsto z_{13},$$
$$\langle 0,1\rangle \mapsto z_{21},\quad \langle 1,1\rangle \mapsto z_{22},\quad \langle 2,1\rangle \mapsto z_{23},$$
$$\langle 0,0\rangle \mapsto z_{31},\quad \langle 1,0\rangle \mapsto z_{32},\quad \langle 2,0\rangle \mapsto z_{33},$$

则仿射平面中的 12 条线恰好对应了设计中的 12 个块,所以例 10.6 中的仿射平面实际上就是例 10.15 中的 Steiner 三元系统.

下面简要介绍一下 Hadamard 矩阵以及由这个矩阵所导出的 2-(v,k,λ) 设计.

定义 10.10 设 $H=(h_{ij})$ 是 n 阶矩阵,其中 h_{ij} 是 1 或 -1. 若 $HH^T=nI$,I 是 n 阶单位矩阵,则称 H 为 **Hadamard 矩阵**. 第一行全是 1 的 Hadamard 矩阵称为**规范的** Hadamard 矩阵.

【例 10.16】 令

$$H_1=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\quad H_2=\begin{bmatrix}1 & 1 & -1 & 1\\ 1 & -1 & -1 & -1\\ -1 & -1 & -1 & 1\\ 1 & -1 & 1 & 1\end{bmatrix},$$

$$H_3=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix},$$

则这三个矩阵都是 Hadamard 矩阵,其中 H_1 和 H_3 是规范的.

可以证明,规范的 n 阶 Hadamard 矩阵($n>2$)具有下面的性质:

1. 存在正整数 m,$n=4m$.
2. 从第二行(或列)起,每一行(或列)恰含有 $2m$ 个 1 和 $2m$ 个 -1.
3. 除第一行(或列)以外,任意两行(或列)中恰有 m 个列(或行)全由 1 构成.

定理 10.13　由 n 阶($n \geqslant 8$)规范的 Hadamard 矩阵可以导出一个对称的 2-(v,k,λ) 设计，其中 $v = n-1, k = \frac{n}{2}-1, \lambda = \frac{n}{4}-1$，称为 **Hadamard 设计**.

证　设 H 是 n 阶规范的 Hadamard 矩阵，$n \geqslant 8$. 删除 H 的第一行和第一列，然后用 0 代替所有的 -1 得到 $n-1$ 阶矩阵 $M=(a_{ij})$，如下构造一个对称的 2-(v,k,λ) 设计.

令 $X=\{1,2,\cdots,n-1\}, B_j=\{i \mid i \in X \text{ 且 } a_{ij}=1\}, j=1,2,\cdots, n-1$. 易见 $v=n-1, k=\frac{n}{2}-1$(性质 2). 任取 $i,j \in X$，由性质 3，M 的第 i 行和第 j 行恰有 $\frac{n}{4}-1$ 个 1 处在相同的列上，即恰有 $\frac{n}{4}-1$ 个块含有 i 和 j，从而证明 $\lambda=\frac{n}{4}-1$. ∎

【例 10.17】　设 H 是 Hadamard 矩阵

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix},$$

则对应的相交矩阵和对称的 2-(7,3,1) 设计如下：

$$M=\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{aligned} X &= \{1,2,3,4,5,6,7\}, \\ B &= \{\{2,4,6\},\{1,4,5\}, \\ &\quad \{3,4,7\},\{1,2,3\}, \\ &\quad \{2,5,7\},\{1,6,7\}, \\ &\quad \{3,5,6\}\}. \end{aligned}$$

实际上这个设计是 Fano 平面.

§10.3 编码

先引入编码理论的一些基本概念.

定义 10.11 设 $S=\{x_1,\cdots,x_q\}$ 是字符的集合. 令 $S^n=\{x_1x_2\cdots x_n\mid x_i\in S\}$,则称 S^n 的子集 C 为 S 上的 **q 元码**,对任何 $x\in C$,称 x 为 C 的**码字**.

定义 10.12 设 C 是 S 上的 q 元码. $\forall x,y\in S^n$, $x=x_1x_2\cdots x_n$, $y=y_1y_2\cdots y_n$,令

$$d(x,y)=|\{i\mid x_i\neq y_i,\ 1\leqslant i\leqslant n\}|,$$

称 $d(x,y)$ 为 x 和 y 的**距离**,且称

$$d(C)=\min\{d(x,y)\mid x,y\in C\}$$

为码 C 的**最小距离**.

定理 10.14 设 S 为有穷字符集,则

(1) $\forall x,y\in S^n$, $d(x,y)=0$ 当且仅当 $x=y$;

(2) $\forall x,y\in S^n$, $d(x,y)=d(y,x)$;

(3) $\forall x,y,z\in S^n$, $d(x,y)+d(y,z)\geqslant d(x,z)$.

证 (1) 和 (2) 是显然的.

(3) $d(x,z)$ 是将 x 变成 z 所需要变动的最少位数. 先将 x 变成 y,再进一步将 y 变成 z,则变动的位数 $d(x,y)+d(y,z)$ 不小于 $d(x,z)$. ∎

由于噪音的干扰码字在传输过程中可能会出错. 在接收时可以判断传输过程是否出错的码为**检错码**;不仅能判断是否出错,而且可以纠正差错的码为**纠错码**. 在纠错时通常采用最近距离译码原则.

定义 10.13 (最近距离译码原则) 设 C 是 S 上的 q 元码. 当用 C 发送某个码字时若接收到的是 $y\in S^n$,令 x 是使得 $d(y,x)$ 取得最小值的 C 中码字,则将 y 译作 x. 称这个译码原则为**最近距离译码原则**.

定理 10.15 设 C 是一个 q 元码.

(1) 若 $d(C) \geqslant t+1$,则 C 可以查出任何码字的 t 位错;

(2) 若 $d(C) \geqslant 2t+1$,则 C 可以纠正任何码字的 t 位错.

证 (1) 设 $d(C) \geqslant t+1$. 若码字 x 在传输过程中出错,且出错位数小于等于 t,则接收到的字不可能是 C 中的码字,故可以查错.

(2) 设 $d(C) \geqslant 2t+1$. 若码字 x 经传输后变成 y,且 $d(x,y) \leqslant t$,则对于任何 C 中的码字 $z, z \neq x$,有 $d(z,y)+d(y,x) \geqslant d(z,x) \geqslant 2t+1$,故 $d(z,y) \geqslant t+1$. 由最近距离译码原则应将 y 译作 x. ∎

定义 10.14 设 C 是 q 元码,若 C 包含了 k 个码字,码字的长为 n,且 $d(C)=d$,则称 C 为 (n,k,d) 码.

【例 10.18】 设 $S=\{0, 1, \cdots, q-1\}$, $C=\{x_1,x_2,\cdots,x_q\}$. 其中

$$x_1 = 00\cdots\cdots0,$$
$$x_2 = 11\cdots\cdots1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x_q = (q-1)(q-1)\cdots(q-1)$$

都是 n 位长的码字,则 $d(C)=n$. 称这个码为**重复码**,它是一个 (n,q,n) 码.

一个好的 (n,k,d) 码应该是 n 尽可能的小,k 尽可能的大,d 也比较大. 一般是给定 n 和 d 来确定一个最大的 k.

定理 10.16

(1) 若 C 为 q 元的 $(n,k,1)$ 码,则最大的 k 是 q^n;

(2) 若 C 为 q 元的 (n,k,n) 码,则最大的 k 是 q.

证 (1) $C \subseteq S^n$,令 $C=S^n$,则

$$\forall x,y \in C \text{ 有 } d(x,y)=1 \text{ 且 } |C|=q^n.$$

(2) $\forall x,y \in S^n$,有 $d(x,y) \leqslant n$. 要使 $d(x,y)=n$,必有 x 与 y 的每一位都不相同. 因为第一位不同的取值至多 q 种,所以 $k \leqslant q$. 而例 10.18 的重复码就是一个 (n,q,n) 码. 所以最大的 k 值就是 q. ∎

设 S 是 q 元字符集，$\forall u \in S^n$，r 为正整数，称集合

$$\{v \mid v \in S^n \wedge d(u,v) \leqslant r\}$$

为**中心是 u 半径是 r 的球**.

定理 10.17 在 S^n 中半径为 $r(0 < r \leqslant n)$ 的球恰好包含了

$$\sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

个字.

证 设 u 是球心. 对于给定的 i，$0 \leqslant i \leqslant r$，若字 v 恰好有 i 位与 u 不同，则位的选择为 $\binom{n}{i}$ 种，每一位的字符可能是 $q-1$ 种，i 位有 $(q-1)^i$ 种. 根据乘法法则，不同的字为 $\binom{n}{i}(q-1)^i$ 个. 再对 i 求和就计数了所有落入球内的字. ∎

定义 10.15 设 C 是 q 元码，令

$$\rho(C) = \max\{\min\{d(x,u) \mid u \in C\} \mid x \in S^n\}.$$

称 $\rho(C)$ 为码 C 的**覆盖半径**.

【例 10.19】 设 $q = \{0,1\}$，$n = 3$，$S^n = \{000,001,010,011,100,101,110,111\}$，$C = \{000,111\}$，则 $\rho(C) = 1$.

定理 10.18 一个 q 元 (n,k,d) 纠错码 C 满足

$$|C| \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leqslant q^n. \tag{10.7}$$

证 由定理 10.15 取 $d = 2t+1$. 以每个码字为中心做半径为 t 的球，则所有的球两两不交. 由定理 10.17，每个球内包含了 $\sum_{i=0}^{t} \binom{n}{i} (q-1)^i$ 个字，因此，所有球内的总字数

$$|C| \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

必小于等于 S^n 内的总字数 q^n. ∎

定理 10.18 给出了 (n,k,d) 纠错码字数的一个上界，称为**海明**

界.

【例 10.20】 长为 6 最小距离为 3 的二进制纠错码至多 9 个码字.

证 $n=6,q=2,d=3$. 从而知道 $t=1$,代入定理 10.18 得

$$|C|\sum_{i=0}^{1}\binom{6}{i}(2-1)^i \leqslant 2^6,$$

即

$$|C|\cdot(1+6)\leqslant 2^6.$$

这就推出

$$|C|\leqslant \frac{64}{7}=9\frac{1}{7},$$

即 $|C|\leqslant 9$. ∎

定义 10.16 设 C 是一个 q 元码,若 C 使得 10.7 式中的等号成立,则称 C 是**完美码**.

易见对于一个完美纠错码 C, 以 C 中每一个码字为中心, 以 $(d-1)/2$ 为半径做的球两两不交,并且 S^n 中的每个字恰好落入一个球中. 码 C 的覆盖半径 $\rho(C)=(d-1)/2$.

下面考虑一类广泛应用的码 —— 线性码.

定义 10.17 设 $F_q=\{0,1,\cdots,q-1\}$ 是域,F_q^n 表示 F_q 上的 n 维线性空间. 称 F_q^n 的一个 k 维子空间为 F_q 上的 **k 维线性码**,记作$[n,k]$码.

定理 10.19 设 C 是 F_q 上的$[n,k]$码,则 C 关于向量加法构成群,是 F_q^n 的子群,且

(1) 对于任意 $v\in F_q^n$,v 属于 C 的某个陪集;

(2) C 的每个陪集恰含有 q^k 个向量.

证 易见 F_q^n 构成群. C 是 F_q^n 的子空间,故对向量加法封闭,又 C 是有穷集,由定理 3.11,C 是 F_q^n 的子群. $\forall v\in F_q^n$,$v\in C+v$,且 $|C|=|C+v|$(根据定理 3.20 和 3.21). 由于 C 是 k 维的,存在着 C 的某

个基 $v_1, v_2, \cdots, v_k$，且对任何 $u \in C$，u 可以唯一表成 $v_1, v_2, \cdots, v_k$ 的线性组合. 又由于 $|F_q| = q$，不同的线性组合有 q^k 种. 因此 $|C + v| = |C| = q^k$. ∎

由于线性码 C 构成群，也称线性码 C 为**群码**.

定义 10.18 设 C 是 $[n,k]$ 码，$v_1, v_2, \cdots, v_k$ 是 C 的一组基. 以 $v_1, v_2, \cdots, v_k$ 作为行所构成的矩阵 G 称为 C 的**生成矩阵**.

【例 10.21】 设 $[7,4]$ 码 C 的一组基为 1110000，1001100，0101010，1101001. 那么码 C 中含 $2^4 = 16$ 个码字，且 C 的生成矩阵 G 以及所有的码字是：

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{aligned} C = \{ & 1110000, 1001100, 0101010, 1101001, \\ & 0000000, 0111100, 1011010, 0011001, \\ & 1100110, 0100101, 1000011, 0010110, \\ & 1111111, 0110011, 0001111, 1010101 \}. \end{aligned}$$

例如码字

$$1010101 = 1110000 + 1001100 + 1101001.$$

若对 G 进行一系列初等行变换（两行交换，某一行的 i 倍加到另一行上）可得到标准形的矩阵 G'.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\rightarrow \underset{G'}{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}}.$$

根据线性空间的性质知 1000011,0100101,0010110 和 0001111 也是 C 的一组基,因此 G' 也是码 C 的生成矩阵.

下面考虑编码和译码. 以二进制码为例,假设被编码的信息向量 $u = u_1u_2\cdots u_k, u_i \in \{0,1\}$. 设 C 是 F_2 上的$[n,k]$码,G 是 C 的生成矩阵,那么 $uG = \sum_{i=1}^{k} u_iv_i$ 是 $v_1,v_2,\cdots,v_k$ 的线性组合,其中 $v_1,v_2,\cdots,v_k$ 是C的一组基. 易见uG是C中的码字,称为u的代码. 当G是标准形,即

$$G = [I_k\ A] = \begin{bmatrix} 1 & & & & a_{11} & \cdots & a_{1,n-k} \\ & 1 & & 0 & a_{21} & \cdots & a_{2,n-k} \\ & & \ddots & & & \cdots & \\ 0 & & & 1 & a_{k1} & \cdots & a_{k,n-k} \end{bmatrix}$$

时,u 的代码

$$uG = u[I_k\ A] = u_1u_2\cdots u_ku_{k+1}\cdots u_n,$$

其中 $u_{k+i} = \sum_{j=1}^{k} a_{ji}u_j,\ 1 \leqslant i \leqslant n-k$. 称 $u_1,u_2,\cdots,u_k$ 为信号位,$u_{k+1},u_{k+2},\cdots,u_n$ 为校验位.

【例 10.22】 C 为$[7,4]$码,其生成矩阵是

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix},$$

则对于 $u = u_1u_2u_3u_4$，u 的代码为 $u_1u_2u_3u_4u_5u_6u_7$，其中 $u_5 = u_1 + u_2 + u_3$，$u_6 = u_2 + u_3 + u_4$，$u_7 = u_1 + u_2 + u_4$. u_5, u_6, u_7 是校验位.

再考虑译码. 设 C 为 $[n,k]$ 码. 关于 C 的译码阵列是由 F_2^n 的全体向量构成的 2^{n-k} 行 2^k 列的阵列. 根据定理 10.19，F_2^n 构成群，C 是 F_2^n 的子群且 $|C| = 2^k$. 由 Lagrange 定理(定理 3.26)，C 在 F_2^n 中有 2^{n-k} 个陪集. 译码阵列的每一行由同一陪集的向量构成，其中

第一行由 C 中的全体向量构成，即 $C = \{v_1 = 0, v_2, v_3, \cdots, v_{2^k}\}$；

第二行为 $C + a_1$，其中 a_1 是 $F_2^n - C$ 中具有最少个 1 的向量，即第二行元素为 a_1，$v_2 + a_1$，$v_3 + a_1$，$\cdots$，$v_{2^k} + a_1$；

第三行为 $C + a_2$，a_2 是 $F_2^n - C - (C + a_1)$ 中具有最少个 1 的向量；

……

第 2^{n-k} 行为最后剩下的 2^k 个向量.

称这个译码阵列为 Slepian 译码表. 设发送的码字 $v_i \in C$. 若接收到的是 x，$x \notin C$，$x \in C + a_j$，这时可将 x 译作 $x + a_j$. 不难看出，$x + a_j = (v_l + a_j) + a_j = v_l$，$v_l \in C$，因此 $x + a_j$ 是 C 中的码字. 而由阵列的构成知道 a_j 恰好处在阵列的第一列. 称 Slepian 译码表的第一列为**错误向量**. 如果干扰恰好为第一列的元素，通过这样的译码可以纠正传输中的错误，否则这种译码就会出错.

可以证明这种陪集译码方法是符合最近距离译码原则的. 证明留给读者完成.

【例 10.23】 设 $C = \{0000, 0110, 1001, 1111\}$ 是 $[4,2]$ 码，则关于 C 的 Slepian 译码表如下：

0000	0110	1001	1111
0001	0111	1000	1110
0010	0100	1011	1101
0011	0101	1010	1100

如果接收到的字是 1001，则它是 C 中的码字，在译码时就译为 1001. 如果接收到的字是 1101，不是 C 中的码字，那么从表中查到 1101 所在的行的第一元素为 0010，这时将 1101 译作 $1101 + 0010 = 1111$. 1111 是距离 1101 最近的码字之一. 找到正确的码字，去掉校验位就是信息.

定义 10.19　设 C 为 $[n,k]$ 码，其生成矩阵为 G. 令

$$C^{\perp} = \{v \mid v \in F_q^n \text{ 且 } v \cdot u = 0 (\forall u \in C)\},$$

称 $C^{\perp}$ 为 C 的**对偶码**.

定理 10.20　设 C 为 F_q 上的 $[n,k]$ 码，则 $C^{\perp}$ 是 F_q 上的 $[n,n-k]$ 码.

证　任取 $v_1, v_2 \in C^{\perp}$，$a, b \in F_q$，则对任意的 $u \in C$ 有

$$(av_1 + bv_2) \cdot u = av_1 \cdot u + bv_2 \cdot u = a0 + b0 = 0,$$

所以 $av_1 + bv_2 \in C^{\perp}$，即 $C^{\perp}$ 是 F_q^n 的子空间. 下面证明 $C^{\perp}$ 的维数为 $n-k$.

设 $G = (r_{ij})$ 是码 C 的生成矩阵，对任意的 $v \in C^{\perp}$，$v = v_1 v_2 \cdots v_n$，有

$$\sum_{j=1}^{n} r_{ij} v_j = 0, \quad i = 1, 2, \cdots, k,$$

这是由于 G 的行向量恰为 C 中的码字. 对于 n 个未知数，k 个线性独立方程的齐次线性方程组，其基础解系的维数是 $n-k$，从而证明了 $C^{\perp}$ 的维数为 $n-k$. ∎

定义 10.20　设 C 为 F_q 上的 $[n,k]$ 码，称 $C^{\perp}$ 的生成矩阵 H 为 C 的**校验矩阵**.

【例 10.24】　设 C 是 F_2 上的 $[7,4]$ 码，C 的生成矩阵 G 是

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

设 $v \in C^{\perp}$，$v = v_1 v_2 \cdots v_7$，则根据 $G \cdot v = 0$ 可知

$$\begin{cases} v_1 + v_5 + v_7 = 0, \\ v_2 + v_5 + v_6 + v_7 = 0, \\ v_3 + v_5 + v_6 = 0, \\ v_4 + v_6 + v_7 = 0. \end{cases}$$

不难找到三个线性无关的 v 满足上述方程组，例如 1110100，0111010，1101001. 这样就得到 $C^{\perp}$ 的生成矩阵，也就是 C 的校验矩阵

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

定理 10.21　设 C 为 F_q 上的 $[n,k]$ 码，C 的生成矩阵 G 的标准形是 $[I_k\ A]$，则 C 的校验矩阵 $H = [-A^T\ I_{n-k}]$.

证

$$G = \begin{bmatrix} 1 & & 0 & a_{11} & \cdots & a_{1,n-k} \\ & \ddots & & \cdots & \cdots & \cdots \\ 0 & & 1 & a_{k1} & \cdots & a_{k,n-k} \end{bmatrix}.$$

令

$$H = \begin{bmatrix} -a_{11} & \cdots & -a_{k1} & 1 & & 0 \\ \cdots & \cdots & \cdots & & \ddots & \\ -a_{1,n-k} & \cdots & -a_{k,n-k} & 0 & & 1 \end{bmatrix},$$

则 H 为 $n-k$ 行 n 列矩阵，且行是线性无关的. 任取 H 的第 j 行，G 的第 i 行相乘得

$$(-a_{1j} \cdots -a_{kj} 0 \cdots 1 0 \cdots 0) \cdot (0 \cdots 1 0 \cdots 0 a_{i1} \cdots a_{i,n-k})$$

$= 0 + 0 + \cdots + (-a_{ij}) + 0 + \cdots + 0 + a_{ij} + 0 + \cdots + 0 = 0,$
从而证明 $GH^T = 0$，故 H 是码 C 的校验矩阵. ∎

【例 10.25】 按照定理 10.21，对例 10.24 中的码 C 来说，从生成矩阵 G 到校验矩阵 H 的求解过程可以图示如下：

$$\underset{G}{\begin{bmatrix}1000101\\0100111\\0010110\\0001011\end{bmatrix}} \to \begin{bmatrix}1000 & 101\\0100 & 111\\0010 & 110\\0001 & 011\end{bmatrix}_{I_4 \quad A} \to \begin{bmatrix}1110 & 100\\0111 & 010\\1101 & 001\end{bmatrix}_{-A^T \quad I_3} \to \underset{H}{\begin{bmatrix}1110100\\0111010\\1101001\end{bmatrix}}.$$

任给定生成矩阵 G(k 行 n 列)，则可以定义一个 F_q 上的 $[n,k]$ 码 C，并可以求得 C 的校验矩阵 H. 反之，任给定校验矩阵 H($n-k$ 行 n 列)，也可以定义 $[n,k]$ 码 C，并求得 C 的生成矩阵 G.

设 H 是 F_q 上的 $n-k$ 行 n 列的矩阵，且是码 C 的校验矩阵. 如下构造线性函数

$$f: F_q^n \to F_q^{n-k},$$

$$f(x_1 \cdots x_n) = H\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix},$$

则对任意的 $x_1\cdots x_n, y_1\cdots y_n \in F_q^n$ 有

$$f(x_1\cdots x_n + y_1\cdots y_n) = H\begin{pmatrix}x_1+y_1\\ \vdots\\ x_n+y_n\end{pmatrix} = H\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} + H\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$$
$$= f(x_1\cdots x_n) + f(y_1\cdots y_n).$$

这就证明 f 是群 F_q^n 到群 F_q^{n-k} 的同态映射，且

$$\ker f = \{v \mid v \in F_q^n \text{ 且 } f(v) = 0\}.$$

设 $v = x_1x_2\cdots x_n$，则

$$f(v) = 0 \Leftrightarrow Hv = 0 \Leftrightarrow H\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = 0$$

$$\Leftrightarrow (x_1\cdots x_n)H^T = 0 \Leftrightarrow x_1\cdots x_n \in (C^\perp)^\perp.$$

而 $C \subseteq (C^{\perp})^{\perp}$，因为每个 C 中向量垂直于 $C^{\perp}$ 中向量. 又由于 $(C^{\perp})^{\perp}$ 的维数是 $n-(n-k)$，所以有 $(C^{\perp})^{\perp}=C$，从而推出

$$x_1x_2\cdots x_n \in \ker f \Leftrightarrow x_1x_2\cdots x_n \in C.$$

【例 10.26】 设码 C 的校检矩阵为

$$H=\begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix},$$

定义函数

$$f: Z_2^7 \to Z_2^3,\ f(x_1\cdots x_7)=H\begin{pmatrix}x_1\\ \vdots\\ x_7\end{pmatrix},$$

则对于任意 $x_1\cdots x_7 \in \ker f$ 满足

$$\begin{cases}x_2+x_3+x_4+x_5=0,\\x_1+x_3+x_4+x_6=0,\\x_1+x_2+x_4+x_7=0.\end{cases}$$

向量 $x_1\cdots x_7$ 可以是：1000011，0100101，0010110，0001111，从而得到 C 的生成矩阵

$$G=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}.$$

根据定理 10.21 以及例 10.25 也可以得到从校验矩阵直接求生成矩阵的另一种方法. 不难验证这两种方法所求得的码 C 是同一个码.

下面讨论一种广泛使用的线性码——Hamming 码.

定义 10.21 设 r 是正整数，H 为 r 行 (2^r-1) 列矩阵，列是 F_2^r 中的全体非零向量. 以 H 为校验矩阵的码称为 **Hamming 码**，记作 $H(r,2)$ 码.

【例 10.27】 设 $r=3$，H 为 3×7 阶矩阵

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

则 Hamming 码 $H(3,2)$ 的生成矩阵

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

且最小距离是 3.

定理 10.22 设 $r \geqslant 2$，则 Hamming 码 $H(r,2)$

(1) 是$[2^r - 1, 2^r - 1 - r]$码；

(2) 最小距离为 3；

(3) 是完美码.

证 (1) 因为 H 是 r 行$(2^r - 1)$列矩阵，所以 $H(r,2)$ 码的对偶码是$[2^r - 1, r]$码，从而证明了 $H(r,2)$ 码是$[2^r - 1, 2^r - 1 - r]$码.

(2) 任取 $H(r,2)$ 码中的码字 x 和 y，$x + y$ 也是该码中的码字，且 $d(x,y)$ 就是 $x + y$ 中 1 的个数. 下面证明 $H(r,2)$ 码中任何非零码字中 1 的个数至少是 3. 假设码字 v 只含一个 1，不妨设 $v_i = 1$. 由 $v \cdot H^T = 0$ 可知 H 的第 i 列必全为 0，与 H 的定义相矛盾. 假设 v 含两个 1，不妨设 $v_i = v_j = 1$. 又由 $v \cdot H^T = 0$ 知 H 的每一行的第 i 列和第 j 列的元素必相等，从而推出 H 的第 i 列与第 j 列全等，与 H 的定义相矛盾. 综上所述必有 $d(H(r,2)) \geqslant 3$. 另一方面，H 中总有三列的和为 0. 这说明在 $H(r,2)$ 中存在着恰含三个 1 的码字，所以 $d(H(r,2)) = 3$.

(3) $n = 2^r - 1$，而码字的个数为 2^{n-r}，代入 10.7 式左端得

$$2^{n-r}\left[\binom{n}{0} + \binom{n}{1}\right] = 2^{n-r}(1 + 2^r - 1) = 2^n,$$

从而证明了 Hamming 码是完美码. ∎

下面考虑另一种重要的线性码——循环码.

定义 10.22　设 $C \subseteq F_q^n$ 是线性码. 如果 $\forall v \in C, v = v_1v_2\cdots v_n$，有 $v_nv_1\cdots v_{n-1} \in C$，则称 C 是**循环码**.

【**例** 10.28】　设 C 是[7,3]码，其生成矩阵

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

则码 $C = \{0000000, 1011100, 0101110, 0010111,$
$1001011, 1100101, 1110010, 0111001\}$，
不难验证 C 是循环码.

回顾 §4.3(有限域上的多项式环). 设 F_q 是有限域，令 $F_q[X]$ 是 F_q 上所有多项式的集合，则 $F_q[X]$ 关于域 F 上的多项式加法和乘法构成一个环，称为有限域 F 上的多项式环. 令

$$F_q[X]/(x^n-1) = \{v(x) \mid v(x) \in F_q[X] \text{且} v(x) \text{的次数小于} n\},$$

则 $F_q[X]/(x^n-1)$ 关于模 (x^n-1) 的加法和乘法构成域 F_q 上的模 x^n-1 的多项式环.

设 C 为 $[n,k]$ 循环码，$\forall a \in C, a = a_1a_2\cdots a_n$，作多项式

$$a(x) = a_1 + a_2x + \cdots + a_nx^{n-1}.$$

易见码字 a 和 $a(x)$ 是一一对应的，把与 C 中码字对应的全体多项式构成的集合记为 $\mathscr{C}$.

定理 10.23　设码 $C \subseteq F_q^n$，则 C 是循环码当且仅当

(1) $\forall a(x), b(x) \in \mathscr{C}$，有 $a(x) + b(x) \in \mathscr{C}$，

(2) $\forall a(x) \in \mathscr{C}, \forall r(x) \in F_q[X]/(x^n-1)$ 有 $r(x)a(x) \in \mathscr{C}$，

其中的乘法为模 x^n-1 的乘法.

证　必要性. $\forall a(x), b(x) \in \mathscr{C}$，设

$a(x) = a_1 + a_2x + \cdots + a_nx^{n-1}$, $b(x) = b_1 + b_2x + \cdots + b_nx^{n-1}$，
则 $a_1a_2\cdots a_n, b_1b_2\cdots b_n \in C$. 由于 C 是线性码，必有 $a_1a_2\cdots a_n + b_1b_2\cdots b_n \in C$，因此有

$$a(x)+b(x)=\sum_{i=1}^{n}(a_i+b_i)x^{i-1}\in\mathscr{C}.$$

任取 $a(x)\in\mathscr{C}$,$r(x)\in F_q[X]/(x^n-1)$,设

$a(x)=a_1+a_2x+\cdots+a_nx^{n-1}$, $r(x)=r_1+r_2x+\cdots+r_nx^{n-1}$,
则

$$xa(x)=a_n+a_1x+\cdots+a_{n-1}x^{n-1}.$$

由于 C 是循环码,所以 $a_na_1\cdots a_{n-1}\in C$,从而推出 $xa(x)\in\mathscr{C}$.

同理可证 $x^2a(x),\cdots,x^{n-1}a(x)\in\mathscr{C}$,根据(1)的结论,必有 $r(x)a(x)\in\mathscr{C}$.

充分性. 任取 $a,b\in C$,$t,s\in F_q$. 设

$$a=a_1a_2\cdots a_n,\ b=b_1b_2\cdots b_n,$$

则 $a(x)=a_1+a_2x+\cdots+a_nx^{n-1}$, $b(x)=b_1+b_2x+\cdots+b_nx^{n-1}\in\mathscr{C}$. 由(1)和(2)有

$$t(a_1+a_2x+\cdots+a_nx^{n-1})+s(b_1+b_2x+\cdots+b_nx^{n-1})\in\mathscr{C},$$

从而有 $ta+sb\in C$,即 C 是线性码.

任取 $a=a_1a_2\cdots a_n\in C$,则有

$$a(x)=a_1+a_2x+\cdots+a_nx^{n-1}\in\mathscr{C},$$

取 $r(x)=x$,根据(2)有

$$xa(x)=a_n+a_1x+\cdots+a_{n-1}x^{n-1}\in\mathscr{C},$$

即 $a_na_1\cdots a_{n-1}\in C$. 这就证明了 C 是循环码. ∎

以上定理给出了 $C\subseteq F_q^n$ 为循环码的充分必要条件.

定理 10.24　任取 $f(x)\in F_q[X]/(x^n-1)$,令

$$\langle f(x)\rangle=\{r(x)f(x)\mid r(x)\in F_q[X]/(x^n-1)\},$$

则 $\langle f(x)\rangle$ 对应一个 F_q 上的循环码 C,称 C 为 $f(x)$ **生成的循环码**.

证　任取 $a(x)f(x),b(x)f(x)\in\langle f(x)\rangle$,则有

$$a(x)f(x)+b(x)f(x)=(a(x)+b(x))f(x)\in\langle f(x)\rangle.$$

任取 $a(x)f(x)\in\langle f(x)\rangle$,$r(x)\in F_q[X]/(x^n-1)$,则有

$$r(x)(a(x)f(x))=(r(x)a(x))f(x)\in\langle f(x)\rangle.$$

由定理 10.23，$\langle f(x)\rangle$ 对应于循环码 C. ∎

【例 10.29】 设 $F_2=\{0,1\}$，则

$$F_2[X]/(x^3-1)=\{0,1,x,1+x,x^2,1+x^2,x+x^2,1+x+x^2\},$$

取 $f(x)=1+x$，那么

$$\langle f(x)\rangle=\langle 1+x\rangle=\{0,1+x,1+x^2,x+x^2\},$$

而 $\langle 1+x\rangle$ 对应的循环码是

$$C=\{000,\ 110,\ 101,\ 011\}.$$

定理 10.25 设 C 是 F_q^n 中的非零循环码，则在 $F_q[X]/(x^n-1)$ 中存在着唯一的最高次项系数为 1 的次数最低的多项式 $g(x)$，使得 $\mathscr{C}=\langle g(x)\rangle$ 且 $g(x)$ 是 x^n-1 的因式.

证 令 $g(x)$ 是 $\mathscr{C}$ 中次数最低的非零多项式. 不妨设 $g(x)$ 的最高次项系数为 1. 若不然，由于 F_q 是域，必存在 $a\in F_q$ 使得 $ag(x)$ 的最高次项系数为 1，且 $ag(x)$ 与 $g(x)$ 的次数相等. 易见 $\langle g(x)\rangle\subseteq\mathscr{C}$. 反之，任取 $b(x)\in\mathscr{C}$，由多项式除法

$$b(x)=f(x)g(x)+r(x),$$

根据定理 10.23 可知 $r(x)=b(x)-f(x)g(x)\in\mathscr{C}$. 因为 $g(x)$ 的次数最低必有 $r(x)=0$. 这就证明了 $b(x)=f(x)g(x)\in\langle g(x)\rangle$. 从而推出 $\mathscr{C}=\langle g(x)\rangle$.

假设有 $h(x)\in F_q[X]/(x^n-1)$，使得 $\mathscr{C}=\langle h(x)\rangle$，且 $h(x)$ 与 $g(x)$ 的次数相等，$h(x)$ 的最高次项系数也是 1. 那么 $g(x)-h(x)\in\mathscr{C}$，且 $g(x)-h(x)$ 的次数比 $g(x)$ 低. 从而推出 $g(x)-h(x)=0$. 这就证明了 $g(x)$ 的唯一性.

由

$$x^n-1=f(x)g(x)+r(x)$$

可知 $r(x)$ 的次数低于 $g(x)$ 的次数. 又由

$$r(x)=-f(x)g(x)(\mathrm{mod}(x^n-1))$$

可知 $r(x)\in\langle g(x)\rangle$. 根据 $g(x)$ 次数的最低性必有 $r(x)=0$. 从而证明 $g(x)$ 是 x^n-1 的因式. ∎

定义 10.23　在一个非零循环码 C 对应的多项式集 $\mathscr{C}$ 中，定理 10.25 中的那个唯一的最高次项系数是 1 的次数最低的多项式 $g(x)$ 称为码 C 的**生成多项式**.

例如在例 10.29 中的码 C 以 $1+x$ 作为它的生成多项式.

【例 10.30】　试找出所有长为 5 的二进制循环码.

解　由

$$x^5-1=(1+x)(1+x+x^2+x^3+x^4)$$

知 x^5-1 的因式有 4 个：

$$1,\ 1+x,\ 1+x+x^2+x^3+x^4,\ x^5-1.$$

分别生成 4 个循环码.下面列出了它们之间的对应关系.

生成多项式 $g(x)$	$\mathscr{C}=\langle g(x)\rangle$	C
1	$F_2[X]/(x^5-1)$	F_2^5
$1+x$	$\mathscr{C}_1=\langle 1+x\rangle$	C_1
$1+x+x^2+x^3+x^4$	$\mathscr{C}_2=\langle 1+x+x^2+x^3+x^4\rangle$	C_2
x^5-1	$\mathscr{C}=\langle x^5-1\rangle$	C_3

其中

$$C_1=\{00000,11000,01100,00110,00011,10001,10100,01010,00101,10010,01001,11110,01111,10111,11011,11101\}$$

称为**偶权码**，即码中的每个码字含偶数个 1.

$C_2=\{00000,11111\}$ 为重复码.

$C_3=\{00000\}$ 为**零码**.

下面的定理确定了循环码的维数和生成矩阵.

定理 10.26　设 C 为循环码，其生成多项式为

$$g(x)=g_1+g_2x+\cdots+g_{r+1}x^r,$$

则 C 的维数是 $n-r$，且 C 的生成矩阵

$$G=\begin{bmatrix} g_1 & g_2 & g_3 & \cdots & g_r & g_{r+1} & 0 & \cdots & & 0 \\ 0 & g_1 & g_2 & g_3 & \cdots & g_r & g_{r+1} & 0 & \cdots & 0 \\ 0 & 0 & g_1 & g_2 & g_3 & \cdots & g_r & g_{r+1} & 0 \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & g_1 & g_2 & \cdots & & g_r & g_{r+1} \end{bmatrix}.$$

证 $g_1 \neq 0$，若不然，$x^{n-1}g(x) = x^{-1}g(x)$ 也是 $\mathscr{C}$ 中的多项式且它的次数为 $r-1$，与 $g(x)$ 的次数最低相矛盾. 因此 G 的 $n-r$ 行线性无关，每行代表的码字多项式为 $g(x), xg(x), \cdots, x^{n-r-1}g(x)$.

任取码字 $a \in C$，设 a 对应的多项式为 $a(x)$. 由于 $g(x)$ 是码 C 的生成多项式，根据定理 10.25 的证明可知必有 $t(x)$ 使得

$$a(x) = t(x)g(x),\ t(x) = t_1 + t_2x + \cdots + t_{n-r}x^{n-r-1}.$$

从而得到

$$a(x) = t_1g(x) + t_2xg(x) + \cdots + t_{n-r}x^{n-r-1}g(x).$$

这说明 $a(x)$ 是 $g(x), xg(x), \cdots, x^{n-r-1}g(x)$ 的线性组合，所以 G 是 C 的生成矩阵. ∎

【例 10.31】 设 $C = \{00000, 11000, 01100, 00110, 00011, 10001, 10100, 01010, 00101, 10010, 01001, 11110, 01111, 10111, 11011, 11101\}$，$C$ 的生成多项式是 $1+x$，则 C 的维数为 $5-1=4$，且生成矩阵为

$$G=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

§10.4 编码与设计

在前面几节，我们分别讨论了组合设计与编码理论. 实际上在组合设计与编码之间存在着密切的联系，先看两个例子.

【例 10.32】 考虑 Fano 平面（例 10.10），它的相交矩阵

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix},$$

令 $a_1a_2\cdots a_7$ 是 M 中的一行，然后构造 $b_1b_2\cdots b_7$，使得 $b_i = 1 - a_i, i = 1,2,\cdots,7$. 这样得到的 14 个向量再加上 0000000，1111111 构成集合 C. 易见 C 是循环码，是[7,4]码，也是(7,16,3)码. 每个 M 中的码字恰含三个 1，而任两个不同的行仅有一个公共的 1. 由此不难计算 $d(C)$. 令 $w(x)$ 表示 x 中所含 1 的个数，称为 x 的权，$w(x \cap y)$ 表示 x 和 y 相同的位中含 1 的个数. 那么 $\forall x, y \in C, x \neq y$.

(1) 若 x 与 y 都是 $a_1a_2\cdots a_7$ 形式，则

$$d(x,y) = w(x) + w(y) - 2w(x \cap y) = 3 + 3 - 2 \times 1 = 4;$$

(2) 若 x 与 y 都是 $b_1b_2\cdots b_7$ 形式，则

$$d(x,y) = w(x) + w(y) - 2w(x \cap y) = 4 + 4 - 2 \times 2 = 4;$$

(3) 若 $x = 0, y \neq 0$，或 $x \neq 0, y = 0$，则

$$d(x,y) = 3,4 \text{ 或 } 7;$$

(4) 若 $x = 1, y \neq 1$，或 $x \neq 1, y = 1$，

$$d(x,y) = 3,4 \text{ 或 } 7;$$

(5) 若 x, y 中一个为 $a_1a_2\cdots a_7$，另一个为 $b_1b_2\cdots b_7$ 的形式，则

$$d(x,y) = 3 \text{ 或 } 7.$$

综上所述有 $d(C) = 3$，该码恰好满足等式 10.7，即

$$16\left[\binom{7}{0} + \binom{7}{1}\right] = 2^7,$$

所以码 C 是完美码.

【例 10.33】 设 M 是 Hadamard 设计对应的相交矩阵，

$$M = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix},$$

则以该矩阵的每行作为码字构成一个码，称为 **Hadamard 码** C.

$$C = \{ 0101010, 1001100, 0011001, 1110000, \\ 0100101, 1000011, 0010110\}.$$

C 既不是线性码，也不是循环码，只是一个距离为 4 的纠错码.

一般说来，设 M 为一个对称的 2-$(4t-1, 2t-1, t-1)$ 设计的相交矩阵，可以利用这个矩阵得到一个含有 $8t$ 个码字，字长 $4t$，可以纠 $t-1$ 个错的纠错码. 构造方法如下：记 $v = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

任取 M 的一行 $a_{i1}, a_{i2}, \cdots, a_{i,4t-1}$，令

$$a_i = 1a_{i1}a_{i2}\cdots a_{i,4t-1}, \quad i = 1, 2, \cdots, 4t-1$$

作为码字. 然后做 a_i 的补码 $\overline{a_i}$，即

$$\overline{a_i} = 0\,\overline{a}_{i1}\,\overline{a}_{i2}\cdots\overline{a}_{i,4t-1}, \text{其中} \overline{a}_{ij} = 1 - a_{ij}, \ i = 1, 2, \cdots, 4t-1.$$

令

$$C = \{a_i, \overline{a_i}, 00\cdots0, 11\cdots1 \mid i = 1, 2, \cdots, 4t-1\},$$

则 C 是所求的纠错码. 易见 $|C| = 2(4t-1) + 2 = 8t$，且码字长为 $4t$. 任取 $a_i, a_j \in C$, $i \neq j$，则 a_i, a_j 恰有 $\lambda + 1$ 个公共位是 1，而每个码字总共有 $k+1$ 位是 1，因此

$$d(a_i, a_j) = 2(k+1) - 2(\lambda+1) = 2(k-\lambda) = 2t.$$

类似的分析可知

$$d(\overline{a_i}, \overline{a_j}) = 2t,$$

$$d(a_i, \overline{a_j}) = d(\overline{a_j}, a_i) = 2t,$$

$$d(a_i,00\cdots0) = k + 1 = 2t,$$
$$d(a_i,11\cdots1) = 4t - (k+1) = 2t,$$
$$d(a_i,\overline{a_i}) = 4t.$$

所以 $d(C) = 2t$. C 可以查 $2t-1$ 位错,纠 $t-1$ 位错.

也可以采用别的方法来构造纠错码. 如果 M 是一个 2-$(4t-1, 2t-1, t-1)$ 的 Hadamard 设计所对应的相交矩阵,可以取 M 的每一行作为一个码字来构造码 C,那么这个 Hadamard 码是长为 $4t-1$,含有 $4t-1$ 个码字,距离为 $2t$ 的纠错码. 它可以查 $2t-1$ 位错,纠 $t-1$ 位错.

上面已经看到,对于给定的某些 t- 设计,可以构造相应的纠错码. 相反,对于给定的纠错码,也可以构造相应的 t- 设计.

定理 10.27 如果存在一个完美的长为 n 的二元 t- 纠错码,则存在一个 Steiner 系统 $(t+1)$-$(n, 2t+1, 1)$.

证 设 C 是一个完美的长为 n 的二元 t- 纠错码. 任取 $a \in F_2^n$, $w(a) = t+1$,由于 C 是完美的,则存在唯一的 $b \in C$,使得 $d(b,a) \leqslant t$. 这就推出 $1 \leqslant w(b) \leqslant 2t+1$. 又由于 C 是 t- 纠错码,故 $d(b,0) \geqslant 2t+1$,即 $w(b) \geqslant 2t+1$. 从而得到 $w(b) = 2t+1$. 根据 $d(b,a) \leqslant t$ 以及 b 的唯一性可以断定 b 覆盖 a,即对 a 中为 1 的位,b 中相应的位也为 1,b 是唯一覆盖 a 的码字. 令 B 是块的集合,X 是点的集合,其中

$$X = \{1, 2, \cdots, n\}.$$

令 C 中所有权是 $2t+1$ 的码字构成集合 S. 若 $|S| = m$,则 $\forall b_j \in S$ $(j = 1, 2, \cdots, m)$,将码字 b_j 的第 i 位的位号记作 $i (i = 1, 2, \cdots, n)$,并取 b_j 中所有为 1 的位的位号构成块 B_j. 即当 $b_j = b_{j1}b_{j2}\cdots b_{jn}$ 时,则 $B_j = \{i \mid b_{ji} = 1 \text{ 且 } i = 1, 2, \cdots, n\}$ 并且令 $B = \{B_1, B_2, \cdots, B_m\}$. 例如 $n = 7$, $t = 1$, $b_1 = 1101000$ 是 S 中的码字,那么 $B_1 = \{1, 2, 4\}$ 是与 b_1 相对应的块.

任取 X 的 $t+1$ 元子集 $T = \{l_1, l_2, \cdots, l_{t+1}\}$,令

$$a = a_1a_2\cdots a_n,$$

其中

$$a_i = \begin{cases} 1, & i \in T, \\ 0, & \text{否则}. \end{cases}$$

那么 $a \in F_2^n$，且 $w(a) = t + 1$. 根据刚才的分析，必存在唯一的 $b_j \in S$，$w(b_j) = 2t + 1$，使得 b_j 覆盖 a. 换句话说，存在唯一的块 $B_j \in B$，使得 $T \subseteq B_j$. 易见 $|B_j| = 2t + 1$. 这就证明 X 和 B 构成一个 $(t + 1)$-$(n, 2t + 1, 1)$ 设计，即 Steiner 系统 $(t + 1)$-$(n, 2t + 1, 1)$. ∎

【例 10.34】 设

$C = \{$ 1000011, 0100101, 0010110, 0001111,
0011001, 0101010, 1001100, 0110011,
1010101, 1100110, 1110000, 1101001,
1011010, 0111100, 0000000, 1111111$\}$

是一个长为 7 的完美的二元 1- 纠错码，则

$S = \{$ 1000011, 0100101, 0010110, 0011001,
0101010, 1001100, 1110000$\}$.

相对应的 Steiner 系统的点和块的集合是

$X = \{1, 2, 3, 4, 5, 6, 7\}$,

$B = \{ \{1, 6, 7\}, \{2, 5, 7\}, \{3, 5, 6\}, \{3, 4, 7\}, \{2, 4, 6\}, \{1, 4, 5\}, \{1, 2, 3\}\}$.

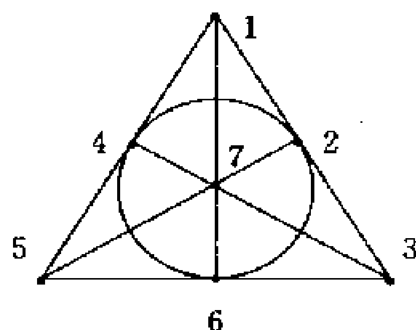


图 10.8

实际上这个 Steiner 系统就是图 10.8 中的 Fano 平面.

习 题 十

1. 构造一个 5 阶的拉丁方.

2. 证明定理 10.1 的(1) 和(2).

3. 在仿射平面 $AP(Z_7)$ 中确定过点(2,5) 且平行于线 $y = 4x + 6$ 的线方程.

4. 构造四个两两正交的 5 阶拉丁方.

5. 构造两个 15 阶的正交拉丁方.

6. 设 $x = \{1,2,3,4,5\}$, $B = \{\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,3,4,5\},\{2,3,4,5\}\}$.

(1) X 与 B 是否构成 2-(v,k,λ) 设计?如果是,确定 v,k,λ 的值,并给出相交矩阵;

(2) X 与 B 是否构成 3-(v,k,λ) 设计?如果是,确定 v,k,λ 的值;

(3) X 与 B 是否构成 Steiner 系统 t-$(v,k,1)$?如果是,确定 v,k 和 t 的值.

7. 证明不存在 Steiner 系统 3-(11,6,1).

8. 证明不存在 2-(v,k,λ) 设计满足 $v = 5, k = 3, \lambda = 2, b = 7, r = 4$.

9. 设 X,B 构成一个 Steiner 三元系统,确定当 $v = 9$ 时的 b 和 r.

10. 试构造一个 21 个点的 Steiner 三元系统.

11. 证明存在着 2-$(v, v-1, v-2)$ 设计.

12. 对下面给定的 n,k,d,能否构成二进制的(n,k,d) 纠错码?如果能,请给出这个码;如果不能,说明理由.

(1) $n = 6$, $k = 2$, $d = 6$;

(2) $n = 8$, $k = 30$, $d = 3$.

13. 设 C 是码字 11010000,11100100,10101010 循环移位加上 00…0 和 11…1 构成. 证明 C 是(8,20,3) 纠错码,且 $d(C) = 3$.

14. 设 C 为线性码,其生成矩阵 G 给定如下,将 G 化成标准形. 求出 C 中所有的码字以及 C 的校验矩阵 H.

(1) $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$;

(2) $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$.

15. 设 C 是二进制线性码,对任意的 $x = x_1x_2\cdots x_n \in C$,令 $x' = x_1x_2\cdots x_nx_{n+1}$,其中 $x_1 + x_2 + \cdots + x_n + x_{n+1} = 0$. 证明 $C' = \{x' \mid x \in C\}$ 也是线性码.

16. 设C_1,C_2是长为n的二进制线性码，证明$C=\{x+y|x\in C_1 \wedge y\in C_2\}$也是长为$n$的二进制线性码.

17. 证明陪集译码法符合最近距离译码原则.

18. 设二进制线性码C的生成矩阵

$$G=\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix}.$$

求关于C的Slepian译码表.若接收到的字是11111和01011，则分别将它们译为哪个码字？

19. 求二进制的Hamming码$H(4,2)$的校验矩阵H及生成矩阵G，并确定码字长和码的维数.

20. 设$f(x)$是F_2上的多项式，且

$$f(x)=x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1).$$

(1) 确定所有长为7的循环码；

(2) 求出这些码的生成矩阵及维数.

第十一章　组合最优化问题

在前面几章里我们讨论了有关组合存在性、组合计数、组合枚举和组合设计的问题，本章将涉及到组合最优化的问题. 先给出有关组合优化问题的一般概念，然后讨论一些优化问题的解.

§11.1　组合优化问题的一般概念

先看一些例子.

【例 11.1】　巡回售货员问题

设有 n 个顶点的完全图 $G=\langle V,E,W\rangle$，其中 $V=\{1,2,\cdots,n\}$ 是 n 个城市的集合，E 是连接这些城市的道路的集合，W 是道路的长度的集合，$c_{ij}\in W$ 表示从城市 i 不经过其它城市而直接到达城市 j 的道路长度. 易见 $c_{ij}=c_{ji}$. 巡回售货员问题就是要从 G 中找一条经过所有的城市并且每个城市只经过一次的最短回路.

设 $i_1i_2\cdots i_n$ 是 $1\ 2\cdots n$ 的一个排列，则巡回售货员问题可以表示为：

$$\min\left(\sum_{k=1}^{n-1}c_{i_ki_{k+1}}+c_{i_ni_1}\right),\tag{11.1}$$

$$i_1i_2\cdots i_n\text{ 是 }1\ 2\cdots n\text{ 的排列}.\tag{11.2}$$

其中 11.1 式可以称为**目标函数**. 11.2 式称为**约束条件**. 这是一个在满足约束条件的情况下使目标函数达到最小的优化问题.

【例 11.2】　钱的分配问题

有 m 元钱用来从事 n 项事业. 已知对第 i 项事业投入 x 元钱以后的经济效益是 $f_i(x)$ 元. 问如何分配这 m 元线才能得到最大的经济效益?

这个分配问题可以表述为：

$$\max \sum_{i=1}^{n} f_i(x_i), \qquad \text{目标函数.}$$

$$\sum_{i=1}^{n} x_i = m, \qquad \text{约束条件.}$$

$$x_i \geqslant 0, i = 1,2,\cdots,n$$

这是一个在满足约束条件的情况下使目标函数达到最大的优化问题.

【例 11.3】 背包问题

一个徒步旅行者准备随身携带一个背包.有许多种东西可以放入背包,每种东西都有一定的重量和价值.他希望在背包的总重量不超过某个数的条件下使得所装入的东西具有最大的价值.问应该怎样选择装入背包的东西?

设有 n 种东西可以装入背包,w_j 是第 j 种东西的重量,v_j 是它的价值,x_j 是装入背包中的第 j 种东西的个数.设 $b > 0$ 是背包总重量的最大值,则背包问题可以表示为:

$$\max \sum_{j=1}^{n} v_j x_j, \qquad \text{目标函数.}$$

$$\sum_{j=1}^{n} w_j x_j \leqslant b, \qquad \text{约束条件.}$$

x_j 为非负整数

在优化问题中,如果目标函数和约束条件都是线性函数,则称这种问题为**线性规则**问题.若在线性规则问题中限制 x_j 是非负整数,则称为**整数规划**问题,背包问题是整数规划问题.若再限定 x_j 只能取 0 或 1,则称为 **0-1 整数规划问题**.相应的背包问题则称为0-1 背包问题.

【例 11.4】 装箱问题

有 n 个物体,其长度分别为 $a_1, a_2, \cdots, a_n$.要把它们装入长为 l 的箱子,如果只考虑长度的限制,问至少需要多少个箱子?

不妨设每个箱子的长度是 1，设 a_i 是第 i 个物体的长度. 令

$$L = (a_1, a_2, \cdots, a_n),\ 0 < a_i \leqslant 1,\ i = 1, 2, \cdots, n,$$

并称 L 为装箱问题的输入. 设箱子的编号为 $B_1, B_2, \cdots, B_m$，其中 B_m 是最后一个非空的箱子. 我们把在箱子 B_j 中装入的所有物体的长度之和叫做 B_j 的容量，记作 $c(B_j)$，而把 B_j 的剩余空间 $1 - c(B_j)$ 叫做 B_j 的空隙. 那么装箱问题可以表示为：

$$\min \quad m, \qquad \text{目标函数.}$$

$$\sum_{i=1}^{n} a_i = \sum_{j=1}^{m} c(B_j),\ c(B_j) \leqslant 1, \qquad \text{约束条件.}$$

上述例子中的问题都是组合最优化问题. 一般说来，一个组合最优化问题应该给出下述参数：

X 有穷的变量集合；

Y 有穷的值的集合；

$f(x)$ 目标函数；

G 约束条件的集合.

一个组合优化问题的解是对变量集 X 的一组赋值 φ: $X \to Y$，并且在满足 G 中约束条件的前提下使得目标函数 $f(x)$ 取得最大（或最小）值.

通常一个组合优化问题的解可能不是唯一的，即可以同时存在着多个满足约束条件的赋值使得目标函数达到最大（或最小）值，但目标函数所达到的最大（或最小）值总是唯一的.

在对组合优化问题做一般性讨论时可以只考虑使目标函数取得最大值的情况，即所谓极大化的组合优化问题. 因为任何极小化的组合优化问题都可以化为极大化的组合优化问题. 设有一个极小化组合优化问题 P_1 描述如下：

$$\min f(x), \qquad \text{目标函数.}$$

$$\left.\begin{aligned} & g_i(x) = 0, \quad i = 1, 2, \cdots, m, \\ & h_j(x) \leqslant 0, \quad j = 1, 2, \cdots, k, \end{aligned}\right\} \qquad \text{约束条件.}$$

那么可以构造一个相应的极大化组合优化问题 P_2:

$$
\begin{array}{lll}
\max\ -f(x), & & \text{目标函数.} \\
g_i(x)=0, & i=1,2,\cdots,m, & \\
h_j(x)\leqslant 0, & j=1,2,\cdots,k, & \text{约束条件.}
\end{array}
$$

易见问题 P_2 的一组解也是问题 P_1 的一组解. 相反,任何极大化的组合 优化问题也可以化为极小化的组合优化问题. 极大化组合优化问题与极小化组合优化问题是可以相互转化的.

§11.2 网络的最大流问题

定义 11.1 一个**有向网络** $D=\langle V,E,W\rangle$ 是一个带权的有向图. 其中 V 是顶点集,$s,t\in V$,s 只有出去的边,称为**源**,t 只有进来的边,称为**漏**. 对任意的边 $e\in E$,有一个非负整数作为 e 的权.

设有向网络 $D=\langle V,E,W\rangle$ 代表一个运输网络. 每个顶点代表城市. 边 $\langle i,j\rangle$ 代表从 i 到 j 的公路,边的权表示这条公路单位时间通过的最大运输量,称为这条边的容量,记作 c_{ij}. 怎样制定运输规划而使得总的流量达到最大?换句话说,使得从 s 出发的总运输量达到最大?这个问题就是网络的最大流问题,可以形式化描述如下:

令 c_{ij} 表示边 $\langle i,j\rangle$ 的容量,x_{ij} 表示边 $\langle i,j\rangle$ 的流量,那么有

$$
\max \quad \sum_j x_{sj}, \tag{11.3}
$$

$$
\sum_j x_{ij}=\sum_k x_{ki},\quad i\neq s,t, \tag{11.4}
$$

$$
0\leqslant x_{ij}\leqslant c_{ij}, \tag{11.5}
$$

其中 11.3 式是目标函数,表示从源 s 流出的流量. 11.4 式和 11.5 式是约束条件,表示从任何结点(除源和漏以外)流出该结点的流量应该 等于流入该结点的流量,即流量守恒;此外,每条边上的流量不应超过边的容量.

由于约束条件和目标函数都是线性的,最大流问题是线性规划

问题.

满足约束条件的解是所有 x_{ij} 的集合，称为一个 $\langle s,t\rangle$ **流**，而 $\sum_j x_{sj}$ 称为这个流的值.

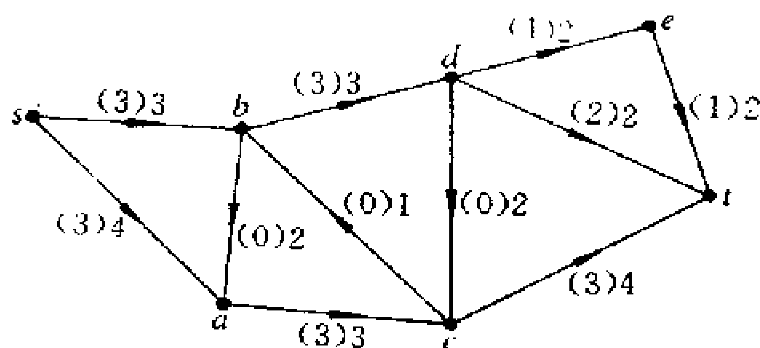


图 11.1

图 11.1 就是一个最大流问题的实例，其中 $V=\{s,a,b,c,d,e,t\}$，边上的数代表这条边的容量，而括号内的数代表流量. 易见 $x_{ij}\leqslant c_{ij}$，$i,j\in V$ 且 $\langle i,j\rangle\in E$. 该实例的解是

$$x_{sb}=3,\ x_{sa}=3,\ x_{ba}=0,\ x_{ac}=3,\ x_{cb}=0,\ x_{bd}=3,$$
$$x_{dc}=0,\ x_{de}=1,\ x_{et}=1,\ x_{dt}=2,\ x_{ct}=3.$$

最大流的值为 6.

在最大流问题中若边 $\langle i,j\rangle$ 满足 $x_{ij}=c_{ij}$，则称这条边是**瓶颈**，而瓶颈是制约进一步提高网络最大流的关键. 图 11.1 中的 $\langle s,b\rangle$，$\langle a,c\rangle$，$\langle d,t\rangle$，$\langle b,d\rangle$ 四条边是瓶颈.

定义 11.2　设 $D=\langle V,E\rangle$ 是有向图，V 的一个划分 $\langle S,T\rangle$ 称为 D 的一个**切割**. 如果 $s\in S$，$t\in T$，则称该切割是分离 s 和 t 的切割，记为 $\langle s,t\rangle$ **切割**.

定义 11.3　设 $D=\langle V,E,W\rangle$ 是一个有向网络，$\langle S,T\rangle$ 是 D 的一个切割，则该切割的容量

$$C(S,T)=\sum_{i\in S}\sum_{j\in T}c_{ij},$$

在所有的 $\langle s,t\rangle$ 切割中容量最小的切割称为**最小切割**.

例如图 11.1 中，$\langle\{s,a,b\},\{c,d,e,t\}\rangle$ 是一个 $\langle S,T\rangle$ 切割，其中 $S=\{s,a,b,\}$，$T=\{c,d,e,t\}$，其容量为

$$C(S,T)=c_{bd}+c_{ac}=6.$$

关于有向网络的流的值和$\langle s,t\rangle$切割的容量有下面的定理.

定理 11.1 在一个有向网络中,任何$\langle s,t\rangle$流的值小于等于任何$\langle s,t\rangle$切割的容量.

证 设所有的x_{ij}构成一个$\langle s,t\rangle$流,$\langle S,T\rangle$是任意的$\langle s,t\rangle$切割.则流的值v满足

$$\begin{aligned}
v &= \sum_j x_{sj} = \sum_j x_{sj} - \sum_j x_{js} \\
&= \sum_{i\in S}\left(\sum_j x_{ij} - \sum_j x_{ji}\right) \\
&= \sum_{i\in S}\sum_{j\in S}(x_{ij} - x_{ji}) + \sum_{i\in S}\sum_{j\in T}(x_{ij} - x_{ji}) \\
&= \sum_{i\in S}\sum_{j\in T}(x_{ij} - x_{ji}) \\
&\leqslant \sum_{i\in S}\sum_{j\in T} x_{ij} \\
&\leqslant \sum_{i\in S}\sum_{j\in T} c_{ij} = C(S,T).
\end{aligned}$$

∎

定理 11.2 在一个有向网络中设$\{x_{ij}\}$是一个$\langle s,t\rangle$流,其值为v,$\langle S,T\rangle$为一个$\langle s,t\rangle$切割,其容量为$C(S,T)$,若$v = C(S,T)$,则$\{x_{ij}\}$是一个最大流且$C(S,T)$是一个最小切割.

证 假设$\{x_{kl}\}$为一个最大的$\langle s,t\rangle$流,其值为v',则$v\leqslant v'$.又设$\langle S',T'\rangle$为一个最小的$\langle s,t\rangle$切割,其容量为$C(S',T')$,则$C(S',T')\leqslant C(S,T)$,由定理 11.1 得

$$v \leqslant v' \leqslant C(S',T') \leqslant C(S,T),$$

又已知$v = C(S,T)$,从而有

$$v = v',\ C(S,T) = C(S',T').$$

∎

定理 11.2 称为网络的最大流最小切割定理.在图 11.1 的有向网络中,一个最小的$\langle s,t\rangle$切割为$\langle \{s,a,b\},\{c,d,e,t\}\rangle$,该切割的容量是 6,而最大流的值也是 6.

定义 11.4 设D为有向网络,$P = \langle i_1,i_2,\cdots,i_k\rangle$是$k$个顶点的

序列，且 $\forall j \in \{1,2,\cdots,k-1\}$ 有 $\langle i_j, i_{j+1}\rangle \in E$ 或 $\langle i_{j+1}, i_j\rangle \in E$，则称 P 为 D 中一条从 i_1 到 i_k 的**链**. 在 P 中，若 $\langle i_j, i_{j+1}\rangle \in E$，则称 $e = \langle i_j, i_{j+1}\rangle$ 为**前向边**；若 $\langle i_{j+1}, i_j\rangle \in E$，则称 $e = \langle i_{j+1}, i_j\rangle$ 为**后向边**.

例如图 11.1 中，$\langle s,a,b,d,t\rangle$ 是 D 中一条从 s 到 t 的链，其中 $\langle s,a\rangle$，$\langle b,d\rangle$，$\langle d,t\rangle$ 是前向边，$\langle b,a\rangle$ 是后向边.

定义 11.5　设 D 为有向网络，P 是 D 中一条从 s 到 t 的链. 如果 P 中任一前向边 $\langle i,j\rangle$ 都有 $x_{ij} < c_{ij}$，任一后向边 $\langle i,j\rangle$ 都有 $x_{ij} > 0$，则称 P 是 D 中一条**流可增加链**.

易见在图 11.1 中不存在流可增加链. 而在图 11.2 中 $\langle s,c,b,t\rangle$ 是一条流可增加链，其中

$$x_{sc} = 2 < 4,\ x_{bc} = 1 > 0,$$
$$x_{bt} = 4 < 5.$$

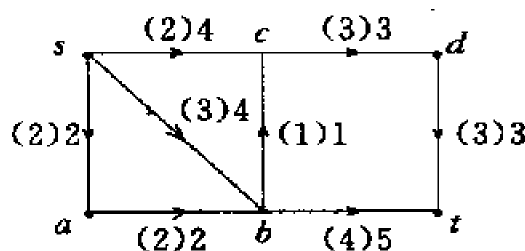


图　11.2

定理 11.3　在有向网络 D 中，一个 $\langle s,t\rangle$ 流是最大流当且仅当不存在从 s 到 t 的流可增加链.

证　设 $D = \langle V,E,W\rangle$.

充分性. 若 D 中不存在从 s 到 t 的流可增加链，令

$$S = \{j \mid j \in V \text{ 且存在从 } s \text{ 到 } j \text{ 的流可增加链}\},$$
$$T = V - S,$$

易见 $s \in S, t \in T$. 对任意 $i \in S, j \in T$，有 $x_{ij} = c_{ij}, x_{ji} = 0$. 否则存在从 s 到 j 的流可增加链，与 $j \in T$ 矛盾. 这就推出 $x_{ij} - x_{ji} = c_{ij}$，所以流值

$$v = \sum_{i\in S}\sum_{j\in T}(x_{ij} - x_{ji}) = \sum_{i\in S}\sum_{j\in T}c_{ij} = C(S,T).$$

由定理 11.2，$\langle s,t\rangle$ 流是最大流.

必要性. 若 $P = \langle s = i_1, i_2, \cdots, i_k = t\rangle$ 是 D 中一条流可增加链. 对 P 中任一前向边 $\langle i,j\rangle$，令 $\delta_{ij} = c_{ij} - x_{ij}$，对 P 中任一后向边 $\langle j,i\rangle$，令 $\delta_{ij} = x_{ji}$. 取 $\delta = \min\{\delta_{i_l i_{l+1}} \mid l = 1,2,\cdots,k-1\}$，则每条 P 上的边

可增加流值 δ(后向边减少流值 δ),与 $\langle s,t\rangle$ 流是最大流矛盾. ∎

根据这个定理可以给出网络最大流的算法.

算法 11.1

输入　有向网络,源为 s,漏为 t,

输出　从 s 到 t 的最大流 $\{x_{ij}\}$.

1. 对所有的 $i,j,x_{ij}\leftarrow 0$;
2. 找一条从 s 到 t 的流可增加链 P. 如不存在,则转 7;
3. 对 P 的每条前向边 $\langle i,j\rangle$,令 $\delta_{ij}=c_{ij}-x_{ij}$;对 P 的每条后向边 $\langle j,i\rangle$,令 $\delta_{ij}=x_{ji}$;
4. 令 $\delta=\min\{\delta_{ij}\}$;
5. 对每个 x_{ij},若 $\langle i,j\rangle$ 为前向边,则 $x_{ij}\leftarrow x_{ij}+\delta$;若 $\langle j,i\rangle$ 为后向边,则 $x_{ji}\leftarrow x_{ji}-\delta$;
6. 转 2;
7. 停止.

【例 11.5】 图 11.3(1) 是一个有向网络. 根据算法 11.1 使用标号的方法求最大流的步骤如下:

初始,令所有的 $x_{ij}=0$,并将 x_{ij} 标记在括号内.

取图中一条流可增加链(粗黑线标出),并增加链上每条边的流,直到网络中不存在流可增加链为止. 各步中的流可增加链,及修改流的过程如图 11.3(2)—(6) 所示.

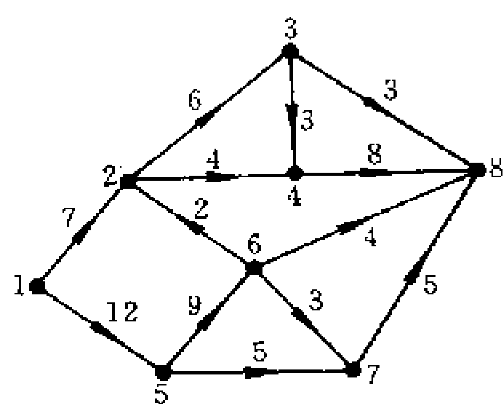
该网络的最大流为下面 x_{ij} 的集合.

$x_{12}=7$, $x_{15}=11$, $x_{23}=5$, $x_{24}=4$, $x_{34}=2$, $x_{38}=3$,

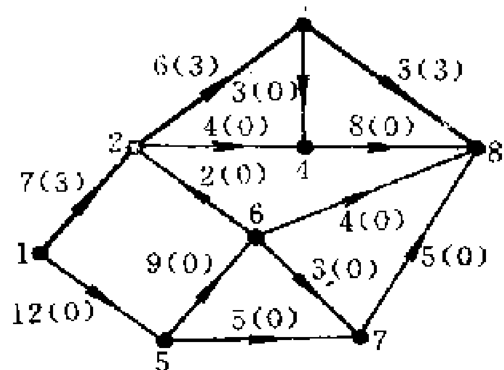
$x_{48}=6$, $x_{56}=6$, $x_{57}=5$, $x_{62}=2$, $x_{67}=0$, $x_{68}=4$, $x_{78}=5$.

定理 11.4 若有向网络的所有边的容量为正有理数,则算法 11.1 将在有限步求出网络的最大流.

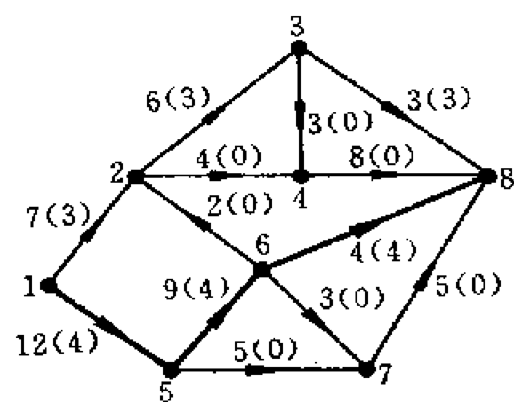
证 若有向网络的所有边的容量为正整数,则算法每寻找一条流可增加链,流的值将增加一个正整数 δ. 在有限步之后,网络中将不存在流可增加链,这时由定理 11.3 达到最大流. 当有向网络的边



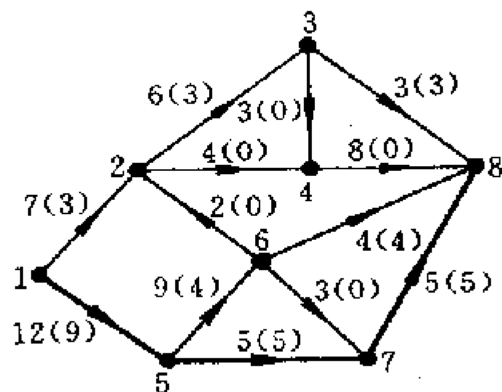
(1)



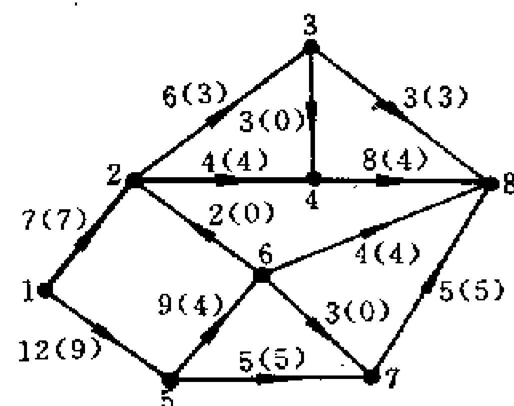
$\delta=3$
(2)



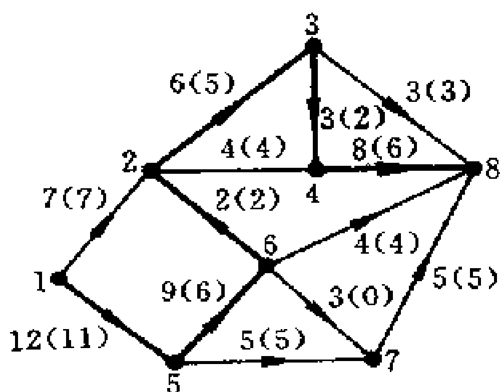
$\delta=4$
(3)



$\delta=5$
(4)



$\delta=4$
(5)



$\delta=2$
(6)

图 11.3

的容量为正有理数$\frac{q_1}{p_1}, \frac{q_2}{p_2}, \cdots, \frac{q_m}{p_m}$时，取 $p_1, p_2, \cdots, p_m$ 的最小公倍数 d，将每条边的容量扩大 d 倍，则每条边的容量变成正整数，在有限步内网络将求出最大流. 然后将每条边的流值除以 d 就得原有向网络的最大流. ▮

算法 11.1 也可以用于多源多漏的有向网络. 设有向网络 $D = \langle V, E, W\rangle$，其中 $s_1, s_2, \cdots, s_m \in V$ 是源，$t_1, t_2, \cdots, t_n \in V$ 是漏. 令 $V' = V \cup \{s, t\}$，且

$$E' = E \cup \{\langle s, s_i\rangle \mid i = 1, 2, \cdots, m\} \cup \{\langle t_j, t\rangle \mid j = 1, 2, \cdots, n\}.$$

规定所有从 s 出发的边和到达 t 的边的容量为 ∞（足够大的正数），那么有向网络 $D' = \langle V', E', W'\rangle$ 的最大流值就是原网络的最大流值. 去掉所增加的结点和边，就得到原网络的最大流.

网络的最大流问题是个线性规划问题的特例，它和许多组合问题有着密切的联系. 下面考虑一个二部图的最大匹配问题.

定义 11.6 设 $G = \langle X, Y, E\rangle$ 是二部图，令

$$V = X \cup Y \cup \{s, t\}, \quad s, t \notin X \cup Y.$$
$$E_1 = \{\langle x, y\rangle \mid x \in X,\ y \in Y,\ \{x, y\} \in E\}.$$
$$E_2 = \{\langle s, x\rangle \mid x \in X\}.$$
$$E_3 = \{\langle y, t\rangle \mid y \in Y\}.$$
$$E' = E_1 \cup E_2 \cup E_3.$$

对任意的 $e \in E'$，若 $e \in E_1$ 则 $w(e) = m$，m 是一个足够大的正整数. 若 $e \in E_2 \cup E_3$，则 $w(e) = 1$. V, E' 和所有的 w 构成有向网络 D，称为 G 的**相关网络**.

引理 1 设 $G = \langle X, Y, E\rangle$ 是二部图，D 为 G 的相关网络，则在 G 的匹配 M 和 D 的整数流之间存在着一一对应，且 D 的流值就是 G 的匹配的边数.

证 任给 D 中一个网络流，若有向边 $\langle x, y\rangle$ 的流量为 1，则边 $\{x, y\} \in M$. 由 D 的构成可知，$\forall x \in X$，流入 x 的流量至多是 1，所以

从 x 出发的有向边中至多有一条流量为 1，这说明至多一条 M 中的边关联到 x. 同理，$\forall y \in Y$，也至多一条 M 中的边关联到 y. 因此，M 构成 G 的一个匹配.

反之，给定 G 中一个匹配 M，令 M 中边的流量为 1，而 G 中其它边的流量为 0. 对于 E_2, E_3 中的边 e，若 e 邻接一条匹配边，则 e 中的流量为 1，否则为 0. 易见对任何 x 和 y，流量守恒且总流的值就是 M 中的边数.

引理 2　设 $G = \langle X, Y, E \rangle$ 为二部图，D 为 G 的相关网络.

$$A \subseteq X,\ B \subseteq Y,\ K = A \cup B,$$

$$S = \{s\} \cup (X - A) \cup B,\ T = \{t\} \cup (Y - B) \cup A,$$

则 K 是 G 的顶点覆盖当且仅当 $\langle S, T \rangle$ 是 D 的一个有限容量的 $\langle s, t \rangle$ 切割，且 $|A \cup B|$ 就是该切割的容量.

证　设 $\langle S, T \rangle$ 是 D 的一个有限容量的 $\langle s, t \rangle$ 切割. 由于 D 是 G 的相关网络，所以 D 中不存在着从 $X - A$ 到 $Y - B$ 的边. 否则这些边就是 S 到 T 的边，且这些边的容量是足够大的正整数 m，与 $\langle S, T \rangle$ 切割的容量是有限的相矛盾. 这就证明了 G 中的边只关联 A 或 B 中的顶点，$A \cup B$ 是 G 的一个顶点覆盖.

反之，若 $K = A \cup B$ 是 G 的顶点覆盖，则 G 中不存在从 $X - A$ 到 $Y - B$ 的边. 因此有

$$C(S,T) = \sum_{x \in A} c_{sx} + \sum_{y \in B} c_{yt} = |A| + |B| = |A \cup B|.$$

这就证明了 $\langle S, T \rangle$ 是 D 的一个有限容量的切割，且切割容量是 $|A \cup B|$. ∎

定理 11.5　设 $G = \langle X, Y, E \rangle$ 是二部图，则 G 中最大匹配的边数等于 G 的顶点覆盖数.

证　令 D 是 G 的相关网络，则在 D 中存在一个最大流. 由引理 1，这个最大流的值等于 G 中最大匹配的边数. 又由定理 11.2，这个最大流对应于 D 中一个最小的 $\langle s, t \rangle$ 切割 $\langle S, T \rangle$，且这个切割的容量

$C(S,T)$ 就等于最大流的值. 因此这个最小切割是有限容量的切割. 由引理 2, $(X-S)\cup(Y-T)=A\cup B(A\subseteq X, B\subseteq Y)$ 是G的一个最小的顶点覆盖, 且顶点覆盖数就是$C(S,T)$. 综上所述, G中最大匹配的边数等于G的顶点覆盖数. ∎

涉及到有向网络的优化问题除了最大流最小切割问题以外, 还有涉及到计划评审技术的关系网络问题. 该网络的每个结点代表一个行为, 如果从 x_i 到 x_j 有一条有向边, 则表示 x_j 必须在 x_i 完成以后才可以开始. 网络中的源 s 表示整个计划的开始, 漏 t 则表示整个计划的结束. 在每个结点的数表示完成这项行为所需要的时间. 我们希望通过这个图 (*PERT* 图, Program Evaluation and Review Technique) 找出每项行为的最早开始时间以及最迟的完成时间, 从而得到整个计划的最早完成时间和关键路径.

涉及到无向网络的优化问题有最短路径问题和最小生成树问题等. 随着计算机网络技术和分布式并行处理的广泛应用和发展, 与通信相关的许多网络分析问题都会提到日程上来, 相应的组合优化技术和算法的研究将会变得更加重要.

习 题 十 一

1. 用标号法求出图 11.4 中每个网络的最大流.
2. 求出图 11.4 中每个网络的最小切割.
3. 求出图 11.5 中每个网络的最大流.
4. 设 $D=\langle V,E,W\rangle$ 是有向网络, $\langle S_1,T_1\rangle$, $\langle S_2,T_2\rangle$ 是D的两个最小切割, 证明$\langle S_1\cup S_2, T_1\cap T_2\rangle$ 也是 D 的最小切割.

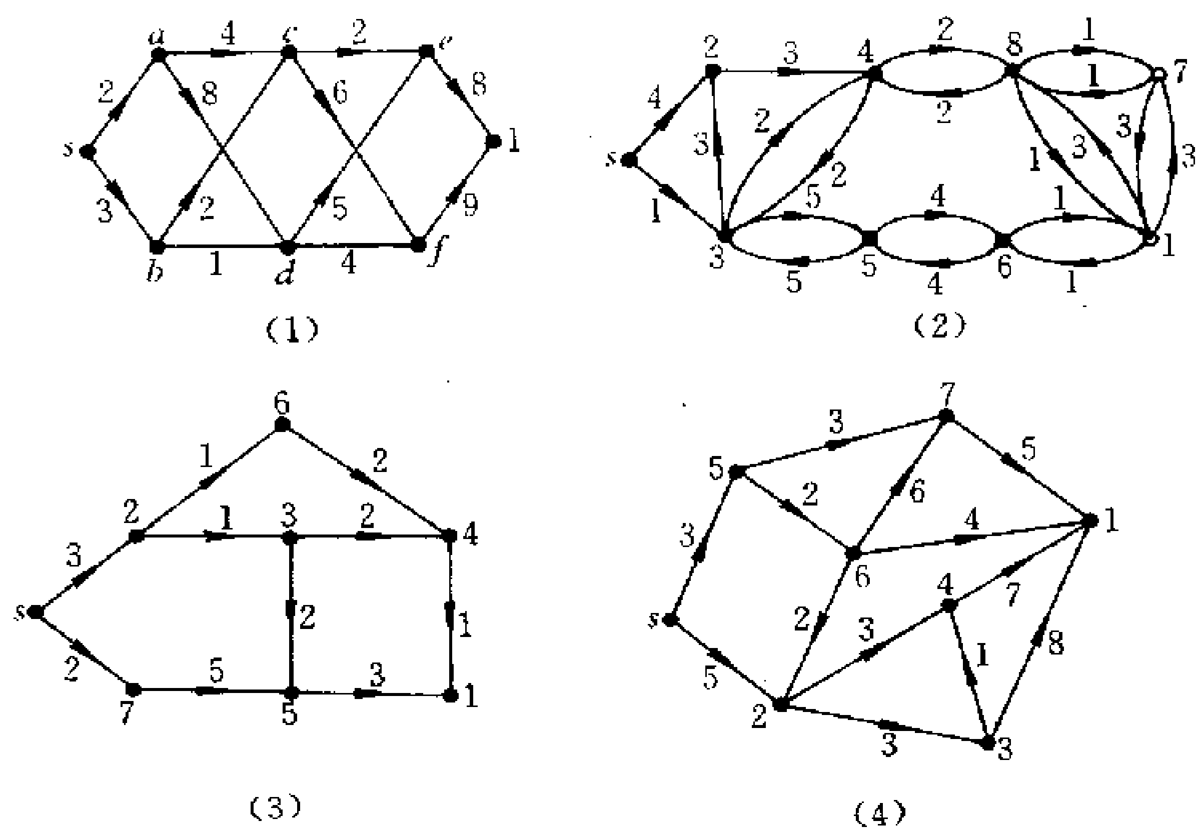


图 11.4

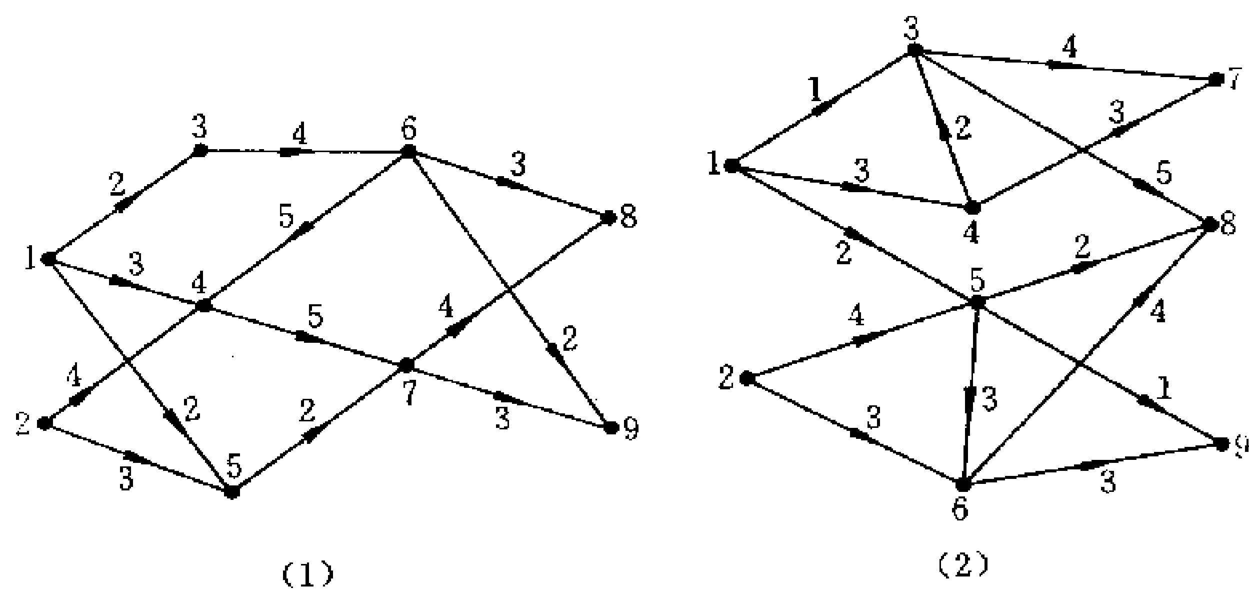


图 11.5

参考书目和文献

[1] 陈进元，屈婉玲，《离散数学》(上)，北京大学出版社，1988

[2] 耿素云，方新贵，《离散数学》(下)，北京大学出版社，1989

[3] 吴品三，《近世代数》，人民教育出版社，1982

[4] 屈婉玲，《组合数学》，北京大学出版社，1989

[5] 卢开澄，《组合数学 算法与分析》，清华大学出版社，1983

[6] 张立昂，《离散数学习题集 抽象代数分册》，北京大学出版社，1990

[7] R. A. Brualdi, Introductory Combinatorics, Elsevier NorthHolland Inc. 1977

[8] D. I. A. Cohen, Basic Techniques of Combinatorial Theory, John Wiley & Sons, 1978

[9] C. L. Liu, Elements of Discrete Mathematics, McCraw-Hill Book Company, 1968

[10] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968

[11] D. K. Ray-Chaudhuri and R. M. Wilson, On t-design, Osaka J. Math, 12, 1975:737—744

[12] E. F. Assmus and H. F. Mattson, Coding and Combinatorics, SIAM Review 16, 1974:349—388

[13] P. Radziszowski, Small Ramsey Numbers, Technical Report AIT-TR-93-009, Rochester Institute of Technology, 1994

术 语 索 引

(注：后面的章或节是该术语第一次出现的章或节)

符号注释

符号	含义
$\forall$	全称量词
$\exists$	存在量词
$\Leftrightarrow$	当且仅当
$\in$	属于
$\notin$	不属于
$\subseteq$	包含
$\subset$	真包含
$\approx$	等势
$\sim$	等价
	同余
	满同态
$\preccurlyeq$	偏序
$\prec$	拟序
$\cong$	同构
$\cap$	集合的交
$\cup$	集合的并
$-$	集合的相对补集
$\oplus$	集合的对称差
	模 n 加
$\otimes$	模 n 乘
$\times$	笛卡儿积
	直积
$\wedge$	合取
	最小上界
	空串
$\vee$	析取
	最大下界
$\varnothing$	空集
N	自然数集(包含 0)
Z	整数集
Z^+	正整数集
Q	有理数集
Q^*	非零有理数集
R	实数集
R^*	非零实数集
R^+	正实数集
C	复数集
	群 G 的中心
$\mathscr{C}$	循环码 C 对应的多项式集
e	单位元
e_l	左单位元
e_r	右单位元
θ	零元
θ_l	左零元
θ_r	右零元
a^{-1}	a 的逆元
$-a$	a 的负元
Σ	有穷字符集
	自动机的输入字符集
P^*	格中命题 P 的对偶命题
Σ^*	Σ 上的所有串的集合
Σ^+	Σ 上的非空串的集合
Γ	自动机的输出字符集
Γ^*	Γ 上的所有串的集合

A^n　集合 A 的 n 阶笛卡尔积

R^n　关系 R 的 n 次幂

S^n　字符集 S 上的长为 n 的串的集合

F^n　域 F 上的 n 维向量空间

x^n　x 的 n 次幂

$\overline{x}$　布尔代数中 x 的补元

B^A　从 A 到 B 的函数集合

T_M　对应于自动机 M 的独异点

I_A　集合 A 上的恒等函数

M^T　矩阵 M 的转置

$C^{\perp}$　码 C 的对偶码

S_n　n 元对称群

A_n　n 元交代群

K_n　完全 n 边形

Z_n　集合 $\{0,1,\cdots,n-1\}$

nZ　集合 $\{nk \mid k\in Z\}$

D_n　n 元集的错位排列数

U_n　n 元集的二重错位排列数

h_n　Catalan 数

$[x]$　x 的等价类或同余类
　　　x 的整数部分

$\lfloor x\rfloor$　不大于 x 的最大整数

$\lceil x\rceil$　不小于 x 的最小整数

$|a|$　a 的阶

$|A|$　有穷集 A 的基数

$|G|$　有限群 G 的阶

$\langle a\rangle$　元素 a 生成的子群

$\langle B\rangle$　子集 B 生成的子群

$A/\sim$　商集

$V/\sim$　商代数

G/H　群 G 关于正规子群 H 的商群

R/D　环 R 关于理想 D 的商环

$\phi(n)$　欧拉函数

$\varphi(A)$　A 在 φ 下的像

$\varphi^{-1}(B)$　B 在 φ 下的完全原像

$P(A)$　A 的幂集

$L(G)$　G 的子群格

$I(L)$　格 L 的理想格

$F[x]$　域 F 上的多项式环

$f(n)$　第 n 个 Fibonacci 数

$c_k(\sigma)$　σ 的轮换表示中的 k-轮换个数

$c(\sigma)$　σ 的轮换表示中的轮换个数

$\beta_0(G)$　图 G 的点独立数

$d(C)$　码 C 的最小距离

$\rho(C)$　码 C 的覆盖半径

$E(A)$　集合 A 的一一变换群

$N(a)$　a 的正规化子

$f\upharpoonright A$　f 限制在 A 上

xRy　表示 $\langle x,y\rangle\in R$

$G\cdot H$　图 G 与 H 的正规积

$\det M$　矩阵 M 的行列式

$AP(F)$　有限域 F 确定的仿射平面

$\ker\varphi$　同态 φ 的核

End G　群 G 的自同态集

Aut G　群 G 的自同构集

Inn G　群 G 的内自同构集

$O(f(n))$　$f(n)$ 的阶

$d(x,y)$　字 x 和 y 的距离

A,B　拉丁方 A 和 B 的并置

$\langle S,T\rangle$　S,T 切割

$C(S,T)$	S,T 切割的容量
$P(n,r)$	n 元集的 r-排列数
$C(n,r)$	n 元集的 r-组合数
$\binom{n}{r}$	n 元集的 r-组合数
$\begin{bmatrix} n \\ r \end{bmatrix}$	第一类 Stirling 数
$\begin{Bmatrix} n \\ r \end{Bmatrix}$	第二类 Stirling 数
BIBD	均衡的不完全区组设计
$[G:H]$	子群 H 在群 G 中的指数
(m,n)	m 和 n 的最大公约数
$n\mid m$	n 整除 m
$n\nmid m$	n 不整除 m
$H\leqslant G$	H 是 G 的子群
$H<G$	H 是 G 的真子群
$H\trianglelefteq G$	H 是 G 的正规子群
$M_1\leqslant M_2$	M_1 是 M_2 的子自动机
$(x)\bmod n$	x 除以 n 的余数
$f: x\mapsto a$	表示 $f(x)=a$
$f: A\to B$	f 是从 A 到 B 的函数
$G=\langle X,Y,E\rangle$	二部图
$D=\langle V,E,W\rangle$	有向网络 D
$f[x]/f[x]$	有限域 F 上模 $f(x)$的多项式环
$[n_1,n_2,\cdots,n_k]$	$n_1,n_2,\cdots,n_k$ 的最小公倍数
$(i_1i_2\cdots i_k)$	k 阶轮换
$R(q_1,q_2,\cdots,q_k;r)$	Ramsey 数
$\binom{n}{n_1\, n_2\cdots\, n_k}$	多项式系数
$\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_k\cdot a_k\}$	多重集
$G_1G_2\cdots G_k$	$\{a_1a_2\cdots a_n \mid a_i\in G_i,\ i=1,2,\cdots,n\}$